2004-06

Radio frequency identification (RFID) for Naval Medical Treatment Facilities (MTF)

Macalanda, Eduardo C.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RADIO FREQUENCY IDENTIFICATION (RFID) FOR NAVAL MEDICAL TREATMENT FACILITIES (MTF)

by

Eduardo C. Macalanda

September 2006

Thesis Advisor:	Dan C. Boger
Associate Advisor:	Douglas E. Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Radio Frequency Identification (RFID) for Naval Medical Treatment Facilities (MTF)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Eduardo C. Macalanda			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The application of Radio Frequency Identification (RFID) technology in hospitals is modest primarily due to cost and policy issues. Similar to the evolution of other electronic technologies, unit costs for components have been dramatically reduced in the past few years. Despite the reduction in costs, RFID technology has not yet achieved the tipping point of economic rationality for adoption at most healthcare organizations. Although the technology has been primarily applied to asset management and supply chain applications, Navy Medicine stands to gain tremendous benefit if this technology could be successfully implemented for staff and patient tracking in addition to inventory management.

The purpose of this thesis was to conduct a review of RFID technology and components that could fit into the Navy Medicine's structure. The study explored the implementation requirements associated with the deployment in other industries that could be used as benchmarks for Navy Medicine implementation. Different technological architectures were described to illustrate the various techniques that could be used for creating the opportunity to automate administration, reduce errors and improve security for both patients and staff.

14. SUBJECT TERMS RFID, implementation, architecture			**15. NUMBER OF PAGES** 145
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RADIO FREQUENCY IDENTIFICATION (RFID) FOR NAVAL MEDICAL TREATMENT FACILITIES (MTF)

Eduardo C. Macalanda
Lieutenant, United States Navy
B.S., Southern Illinois University at Carbondale, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Eduardo C. Macalanda

Approved by: Dr. Dan C. Boger
Thesis Advisor

Dr. Douglas E. Brinkley
Associate Advisor

Dr. Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The application of Radio Frequency Identification (RFID) technology in hospitals is modest primarily due to cost and policy issues. Similar to the evolution of other electronic technologies, unit costs for components have fallen dramatically within the past few years. Despite the reduction in costs, RFID technology has not yet achieved the tipping point of economic rationality for adoption at most healthcare organizations. Although the technology has been primarily applied to asset management and supply chain applications, Navy Medicine stands to gain tremendous benefit if this technology could be successfully implemented for staff and patient tracking in addition to inventory management.

The purpose of this thesis was to conduct a review of RFID technology and components that could fit into the Navy Medicine's structure. The study explores the implementation requirements associated with the deployment in other industries that could be used as benchmarks for Navy Medicine implementation. Different technological architectures are described to illustrate the various techniques that could be used for creating the opportunity to automate administration, reduce errors and improve security for both patients and staff.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am very grateful to the leadership of the United States Navy and the Medical Service Corps for giving me the opportunity to enhance my education and develop my technical knowledge in the field of Information Technology Management. The skills and understanding I gained from my curriculum will help me become a more valuable member of the Navy and the medical community.

My sincere appreciation goes to my professors for their guidance in completing the academic requirements for my curriculum. In particular, I would like to thank Professor Boger and Professor Brinkley for their patience, understanding, and expert advice towards the successful completion of this study.

Most importantly, I thank my family for the support and inspiration they have given me throughout my life and Naval career. I thank my parents, Marcelino and Virginia for the virtues they instilled in me. My wife, Jenny and our children, Josh and Jasmine, were always my source of motivation and support in completing my studies.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ADE	Adverse Drug Event
APS	American Project Services
B2B	Business to Business
CAGE	Commercial and Government Entity
CAT	Computerized Axial Tomography
CATSA	Canadian Air Transport Authority
CCS	Congestion Charging Scheme
CONOPS	Concept of Operations
DBSS	Defense Blood Standard System
DFARS	Defense Federal Acquisition Regulation Supplement
DHHS	Department of Health and Human Services
DLB	Defense Logistics Board
DLE	Defense Logistics Executive
DOD	Department of Defense
EAN	European Archival Network
EPC	Electronic Product Code
ERP	Enterprise Resource Planning
FDA	Food and Dug Administration
GPS	Global Positioning System
GTN	Global Transportation Network
GUI	Graphical User Interface
HERF	Hazards of Electromagnetic Radiation to Fuel

HERO	Hazards of Electromagnetic Radiation to Ordnance
HF	High Frequency
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
ICU	Intensive Care Unit
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identify Friend or Foe
IMC	Information Mediary Corporation
IR	Infrared
ISO	International Standards Organization
ITU	International Telecommunications Union
JAXB	Java Architecture for XML Binding
JCAHO	Joint Commission on Accreditation of Healthcare Organization
JMAR	Joint Medical Asset Repository
JMS	Java Message Service
JTAV	Joint Total Asset Visibility
LAN	Local Area Network
LF	Low Frequency
MQI	Message Queue Integration
MQTT	Message Queue Telemetry Transport
MTF	Military Treatment Facility
NIPRNET	Non-classified Internet Protocol Router Network

NTIA	National Telecommunications and Information Administration
OSD	Office of the Secretary of Defense
OSGI	Open Services Gateway Initiative
PDA	Personal Digital Assistant
PEO EIS	Program Executive Office Executive Information Systems
PPI	Positive Patient Identification
RDBMS	Relational Database Management System
RFID	Radio Frequency Identification
SARS	Severe Acute Respiratory Syndrome
SIPRNET	Secret Internet Protocol Router Network
SGML	Standard Generalized Markup Language
SMF	Service Management Framework
SMS	Short Message Service
UHF	Ultra High Frequency
ULD	Unit Load Device
UPC	Universal Product Code
URL	Uniform Resource Locator
VDC	Venture Development Corporation
VOIP	Voice Over Internet Telephony
WORM	Write Once Read Many
WWW	World Wide Web
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Radio Frequency Identification (RFID) describes a wireless identification technology that communicates data by radio waves. Data is encoded in a chip, which is integrated with an antenna and packaged into a finished tag. RFID tags may be passive that requires installation within close proximity to a reader, or active in which the RFID tag contains a small battery to allow continuous monitoring. RFID technologies offer different options such as memory sizes and forms, and can be read from anywhere within range of the reader.

Today, the application of RFID technologies in hospitals is modest, primarily due to cost issues. Like most electronic technologies, RFID unit costs have fallen dramatically within the past few years, but have not yet achieved the "tipping point" of economic rationality for most healthcare organizations. RFID in healthcare has been restricted primarily to asset management and supply chain applications. In 2003, Jackson Memorial Hospital in Miami reported that it could not account for $4 million worth of equipment and quickly decided to implement RFID tracking [8]. Faced with the similar issue early in 2004, Bon Secours Health System in Richmond, Virginia installed an RFID equipment tracking system to monitor 12,000 pieces of equipment at its three facilities. Additionally, the nursing staff has gained approximately 30 minutes per nurse per shift in time saved not hunting down equipment [27].

Is RFID ready for patient care implementation? Healthcare enthusiasts suggest that one day a tiny RFID tag implanted under human skin could transmit patient information and automatically record a comprehensive record of patient care. If RFID is successfully implemented, hospital staff, drugs, and equipment could be tagged, creating the potential to automate administration, reduce errors and improve security.

B. PURPOSE

The purpose of this thesis is to conduct a review of the currently available RFID technology that could fit into the Navy Medicine network infrastructure and determine the viability of Radio Frequency Identification (RFID) implementation. The initial focus of this thesis will concentrate on the familiarization with the Radio Frequency Identification technology along with its components and available variations. The study will also explore the implementation requirements associated with deployment of RFID in other business sectors that may be considered as benchmarks for Navy Medicine implementation. The study will also look into the existing Department of Defense policies involving RFID implementation at naval medical treatment facilities to determine the likelihood of success for such an endeavor.

C. RESEARCH QUESTIONS

The following questions were used to guide the research and development of this thesis:

1. Is the existing Navy Medicine network infrastructure capable of supporting RFID implementation?
2. What are the needs and requirements for the deployment of RFID within a Military Treatment Facility (MTF) and what are the challenges involved?
3. What would be the benefits associated with the implementation of RFID within Navy Medicine?
4. What would be an ideal architectural design for the deployment of RFID?
5. Would the policies involved in RFID implementation hinder a successful adoption of RFID technology within Navy Medicine?

D. SCOPE OF RESEARCH

This thesis will cover the fundamental features of Radio Frequency Identification and its functional components. It will identify the current standards used for the manufacture and deployment of RFID components for successful implementation. The study will also identify the user requirements involved in optimal implementation along with the challenges associated with the implementation of the technology. It will review

current Radio Frequency Identification architecture and explore the benefits Navy Medicine could gain in implementing the Radio Frequency Identification technology at its medical treatment facilities.

E. METHODOLOGY

The methodology used in this thesis research will consist of the following steps:

1. Conducting a literature search of books, journals, magazines, and material from the World Wide Web regarding the origin and development of the Radio Frequency Identification technology.
2. Identify and describe the functional components and features of the Radio Frequency Identification technology.
3. Explore and evaluate the potential architectural and technical issues crucial to RFID implementation.
4. Identify and evaluate any existing policies related to RFID implementation at naval medical treatment facilities.

THIS PAGE INTENTIONALLY LEFT BLANK

II. GENESIS OF RADIO FREQUENCY IDENTIFICATION

A. WHAT IS RFID?

Radio Frequency Identification (RFID) is a more recent term used to refer to a family of sensing technologies that has been used for more than fifty years. Its origin and association with radio properties can be traced back to the discovery of electromagnetic energy and its early understanding by Michael Faraday during the 1840s [1]. During the same century, James Clerk Maxwell formulated a theory for the propagation of electromagnetic radiation. In the early twentieth century, human beings gained the ability to use radio waves. Before long, a technology that can be used to detect and locate objects relative to its position and speed evolved utilizing the reflection of radio waves gathered. This technology came to be known as radar.

RFID is the combination of radio technology and radar. The technology of radio identification was initially devised for military applications during the Second World War. Radio frequency transponders were installed on Allied aircrafts to identify whether they were friendly or combatant. Consequently, this technology was named Identify Friend or Foe (IFF) which became an indispensable feature on every military and civilian aircraft in operation in the world today [2].

After the development of radio and radar, RFID techniques were further explored in the 1950s. In the late 1960s, radio frequency began to be used for the identification and monitoring of nuclear and other hazardous materials.

Work on RFID began to flourish in the 1970s and 1980s when developers, inventors, companies, universities, and governments actively developed RFID applications in their laboratories. The technology underwent enhancements with the goal of reducing the cost and size in addition to power requirements and communication range. This set the stage for mass market RFID. In the 1990s, millions of RFID tags were incorporated into various applications including toll roads, entry access cards and container tracking. The first mass-market deployment of RFID was in electronic toll collection employed in Oklahoma in 1991 [4]. Since then, technical standards have emerged together with new applications such as RFID in inventory tracking. Table 1

shows how fast RFID is becoming a part of everyday life. RFID is being used as a generic term that can be used to identify objects at a distance using radio frequencies. It has the key advantage of being able to withstand possible signal loss due to obstruction or interference [3].

Decade	Event
1940 - 1950	Radar refined and used. Major World War II development effort. RFID invented in 1948.
1950 - 1960	Early explorations of RFID technology, laboratory experiments.
1960 - 1970	Development of the theory of RFID. Start of applications field trials.
1970 - 1980	Explosion of RFID development. Tests of RFID accelerate. Very early adopter implementations of RFID.
1980 - 1990	Commercial applications of RFID enter mainstream.
1990 - 2000	Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.

Table 1. The Decades of RFID Development.

From: [1]

1. An Emerging Market

According to Venture Development Corporation (VDC), global shipments of RFID systems (hardware, software, and services) reached nearly US$ 965 million in 2002. Venture Development Corporation expects the shipment market to reach US$ 2.7 billion by 2007. In terms of the market as a whole, RFID systems reached $1.3 billion in 2003, and VDC expects the market to experience a compounded annual growth rate of forty-three percent through 2007. The firm Frost and Sullivan is slightly more optimistic with an estimated total of US$ 1.7 billion for RFID systems in 2003, with predictions of US$ 11.7 billion by 2010 [4]. Frost and Sullivan predict that the total RFID-based applications market will experience a compounded annual growth rate of 32.2% [5]. Worldwide sales of RFID integration services are expected to reach US$ 2 billion in 2006

and surpass sales of RFID products in 2007 at approximately US$ 2.8 billion (See Figure 1)

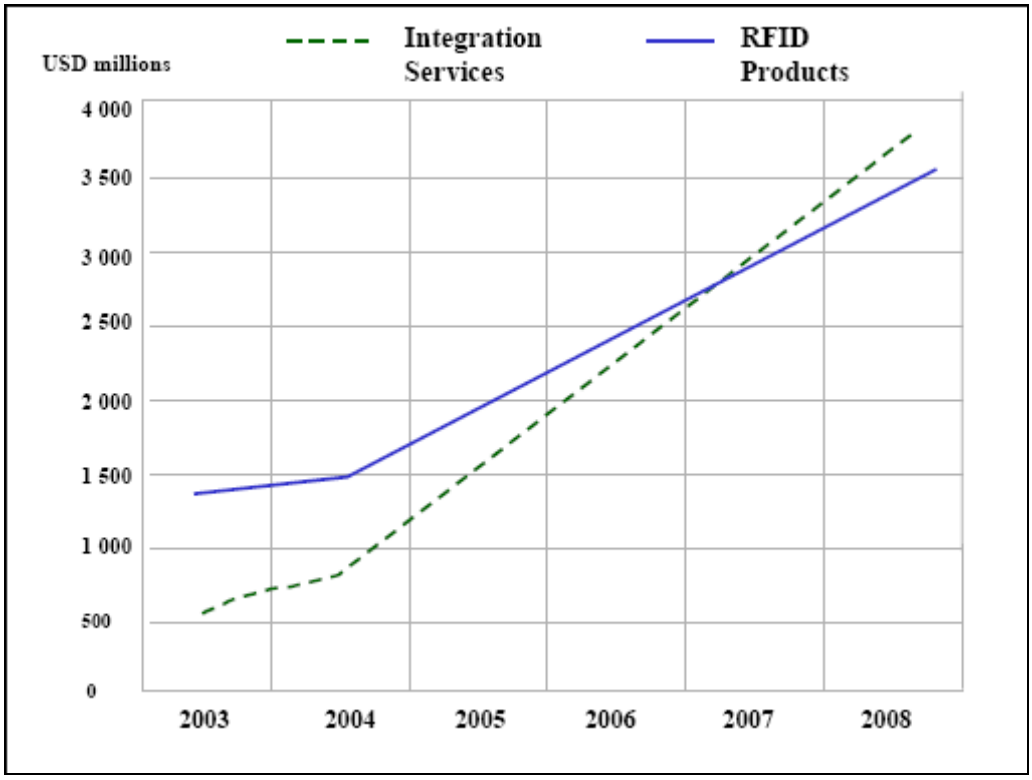


Figure 1. Sales of RFID Products and Integration Services from 2003 to 2008. From: [6]

Most analysts agree that much of the growth experienced in RFID technology has come from traditional and established applications such as security and access control, automobile immobilization, animal tracking, and toll collection. Supply chain management applications are believed to be the most likely drivers of growth in RFID technology in the short term. Eventually, emerging application segments such as electronic product codes and item-level tracking will provide the catalyst for widespread RFID adoption across numerous vertical markets in the medium term.

The Yankee Group predicts that consumer goods manufacturers spent an average of US$ 6.9 million each on RFID in 2004 [7]. Currently, RFID tags for item-level tagging cost from forty cents to ten dollars each and active tags cost between four dollars (US) to hundreds of dollars. There are a number of different predictions with respect to the declining costs of these tags. Some analysts predict that tags will cost as little as five

cents in the near future although the timeline for this event is uncertain. Analysts at Gartner predict that by 2009, the most competitive RFID tags will still cost about 20 cents [8].

B. COMPONENTS OF RFID

Radio frequency identification technology can be seen as a means of identifying a person or object using electromagnetic radiation. Table 2 shows the frequencies that are currently used. These frequencies typically range from 125 kHz (low frequency), 13.56 MHz (high frequency), or 800-960 MHz (ultra high frequency) as represented in Figure 2. RFID enables the automated collection of product, time, place, and transaction information.

RFID systems consist of two main components:

1. Transponder – used to carry data from a tag which is located on or attached to the object to be identified. This normally consists of a coupling element which may include a coil or microwave antenna and an electronic microchip. Figure 3 shows an example of an RFID tag.

2. Reader – used to read the transmitted data emanating from a mobile handheld device or from a fixed device attached to a wall. Readers similar to the one shown in Figure 4 can also be classified as a read only or read/write device.

Regardless of classification, interrogators will always be referred to as a "reader."

Many readers are fitted with an additional interface or middleware to allow the readers to transmit the information it receives forward to another system or intended station such as a personal computer or specified control system [9]. Most of the tags currently used are less than 1/3 mm wide and are typically encapsulated inside a glass or plastic module. Compared with tags, readers are larger, more expensive and power-hungry. In the most common type of system, the reader transmits a low-power radio signal to power the tag. The tag then selectively reflects energy/data back to the reader which now acts are a receiver, communicating its identity and any other relevant information as denoted by the interaction denoted in Figure 5. Most tags are only

activated when they are within the specified interrogation zone of the readers. Outside of that zone, the readers are considered to be in the dormant state.

Frequency Range	LF 125 KHz	HF 13.56 MHz	UHF 868-916 MHz	Microwave 2.45 GHz and 5.8 GHz
Typical Max Read Range (Passive Tags)	< 0.5 m	- 1 m	- 3 m	- 1 m
General Characteristics	Relatively expensive, even at high volumes. Low frequency requires a longer, more expensive copper antenna. Additionally, inductive tags are more expensive than a capacitive tag. Least susceptible to performance degradations from metal and liquids.	Less expensive than inductive LF tags. Relatively short read range and slower data rates when compared to higher frequencies. Best suited for applications that do not require long range reading of multiple tags.	IN large volumes, UHF tags have the potential for being cheaper than LF and HF tags due to recent advances in IC design. Offers good balance between range and performance- especially for reading multiple tags.	Similar characteristics to the UHF tag but with faster rates. A drawback to this band is that microwave transmissions are the mot susceptible to performance degradations due to metal and liquids, among materials. Offers the most directional signal.
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive, E-field coupling	Active tags with integral battery or passive tags using capacitive, E-field coupling
Typical Applications Today	Access control, animal tracking, vehicle immobilizers, POS application, including SpeedPass	Smart Cards, item-level tracking including baggage handling (non-US), libraries	Pallet tracking, electronic toll collection, baggage handling (US)	SCM, electronic toll collection
Notes	Largest install base due to the mature nature of low frequency, inductive transponders	Currently the most widely available high worldwide, due to the mainly relative wide adoption of smart cards	Japan does not allow transmissions in this band. Europe allows 868 MHz whereas the US permits operation at 915 MHz, but at higher power levels	
Data Rate	Slower	-	-	Faster
Ability to read near metal or wet surfaces	Better	-	-	Worse
Passive Tag Size	Larger	-	-	Smaller

Table 2. Different Characteristics of RFID Frequency Ranges. From: [10]

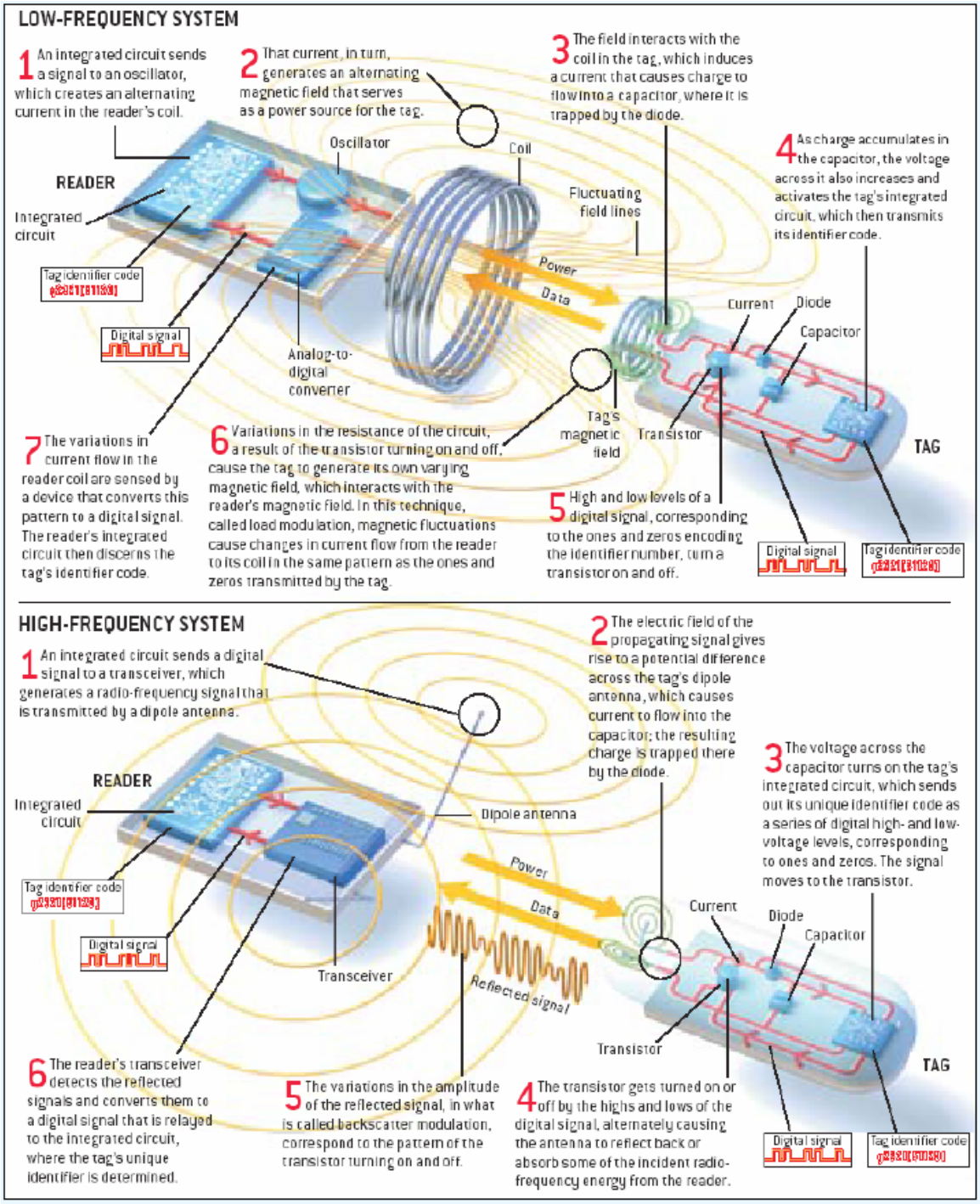


Figure 2. Schematic Representation of RFID Low Frequency and High Frequency From: [14]

Information on the tag can be received and read by the readers. These readers can then be attached to a computer containing the relevant database to update the information as new information about the movement of the tracked objects is received.

Figure 3. The Look of RFID
From: [11]

Figure 4. Symbol XR400 Gen 2 RFID Reader
From: [12]

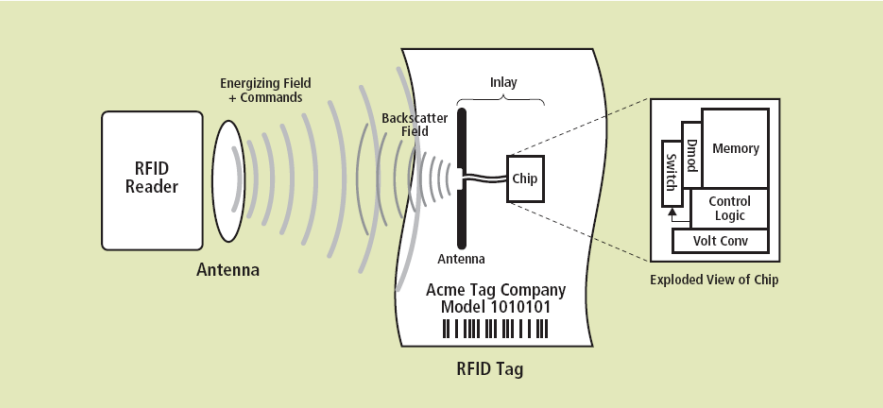


Figure 5. RFID Transponders and Reader Interaction.
From: [13]

Significant amount of media attention is focused on RFID as it pertains to the use of smart tags in consumer sales such as automatic identification and data capture. Many experts predict that this type of RFID tag will be the next generation of the Universal Product Code (UPC) or the traditional bar code currently used on almost all consumer products.

Despite some minor similarities, RFID and the traditional bar code have some very important and fundamental differences. Traditional bar codes identify only a category of products. For example, all Gillette Mach 3 razor blades have the same bar code. Conversely, each packet of these blades would have its own unique identifier that can be transmitted to suitably located readers for monitoring with the use of RFID tags [12]. The Electronic Product Code (EPC) is currently the dominant standard for the data contained in RFID tags for item-level tracking. The EPC can hold more data than a bar code which renders it the capability to become a mini database embedded in every item it is attached to. Another significant advantage that RFID possess over the traditional bar codes is its ability to capture data without the requirement for line of sight communication between the device and the reader. This capability allows for the elimination of physically moving or obtaining physical access to individual items for the purpose of identification and tracking. With the barcode system, objects or items that need to be identified or tracked need to be "seen" at close range by scanners in order to be identified.

RFID is more than the next generation of bar codes. It creates a variety of interfaces that can connect computers directly to individual physical items including human beings. One of the larger RFID networks in the world is the Joint Total Asset Visibility (JTAV) network built by the US military over the last ten years [8]. The JTAV network uses active RFID tags and Global Positioning System (GPS) locators to globally track military supplies. RFID tags have the potential capability of containing information ranging from item location and pricing information to washing instructions, banking details and medical records. Figure 6 shows an example of a message captured by RFID tags. Recent RFID studies have focused on the possibility of implanting RFID tags under the human skin for purposes of authentication, location and transaction [15].

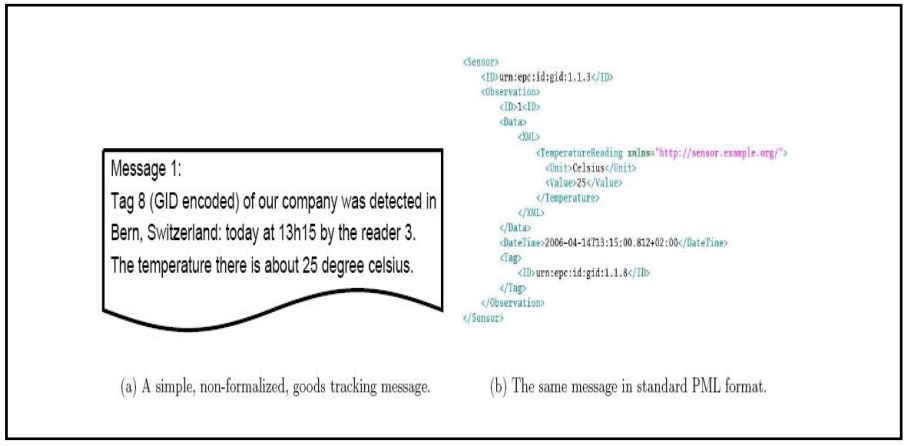


Figure 6. Message Captured by RFID Tags.
From: [13]

1. Types of RFID Systems

One broad classification of RFID tags is whether they contain a microchip. "Chip" tags contain an integrated circuit chip, while "chipless" tags do not. Chipless tags are less expensive to manufacture and may store up to 24 bits of information which provides enough memory for a company's internal use such as on a shop floor or within a warehouse.

In order for a reader to identify all manufactured items, an RFID tag must have enough memory storage to hold a very large ID number designed to identify a massive

number of objects. The reader must also be able to read multiple tags within its range and in close proximity. Chip tag RFID systems enable data, such as a serial number or product code, to be stored and transmitted by portable tags to readers that process the data according to the needs of a particular application [15]. Currently, small chips are able to store 96-bits of data, enough to include a manufacturer's name, a product name and one of trillions of unique numbers that can be assigned to the products.

At the heart of that technology are tiny computer chips smaller than a grain of sand to track items at a short distance. Hitachi, the Japanese semiconductor company, has unveiled a prototype for the next generation of its u-Chip (pronounced mu-chip). The chip is only 0.3 millimeters square, roughly half the size of the smallest RFID chip on the market [16]. It can also hold 128-bits of data.

2. Active and Passive RFID Tags

The working of RFID systems and their features depend on the type of tag system used. There are two main types of RFID tag: active or passive. These tags differ from each other depending on whether they have their own power system to support its operation [9].

Active RFID tags have both an on-tag power source and an active transmitter that allow it to offer superior performance. Because they are connected to their own battery, they can be read at a much higher range from several kilometers away; however, active RFID tags tend to be larger and more expensive. Active RFID tags are well-suited for the manufacturing industry that involved tasks such as tracking components on an assembly line or for logistics, primarily where the tag device will be reused.

Passive tags have no power source and no on-tag transmitter. The lack of these on-tag resources limits their transmission range to less than ten meters and makes them sensitive to regulatory and environmental constraints. On the other hand, they have the most potential for lowest cost, making them suited for mass single-use applications.

C. APPLICATION DOMAINS

1. Transport and Logistics

One of the most promising areas for the application of RFID is public transport. RFID was first deployed for collecting fares on toll highways. Public transport companies are continuing to suffer losses due to the time-consuming and expensive sale of travel passes and tickets through automatic dispensers or in vehicles. Electronic fare management systems using RFID have been fairly successful in reducing overhead for transport companies and in facilitating travel for commuters. Typically, such systems use contactless smart cards, which last for about 10 years and are not easily damaged by liquid, dust or temperature fluctuations. In Europe, the Parisian mass transit authority uses RFID-based automated fare collection technology. The mass transit system in Seattle, Washington uses a Philips RFID contactless smart card for fare collection. In 2004, Transport for London (TfL) announced plans to spend up US$ 65.3 million on new digital enforcement technologies for the Congestion Charging Scheme (CCS) for vehicles, which will most likely include radio frequency identification (RFID) tags for the identification of number plates. But the Asia-Pacific region remains a leader in this field. Korea's "bus card" based on RFID has been around since 1997. Thailand's Bangkok subway uses RFID contactless round token system for individual trips as well as a contactless card system (i.e., one which does not require the contact with a reading machine) for regular travelers. In Tokyo, even taxi drivers have begun using RFID to facilitate their operations. A trial of the payment system was launched in October 2004 and consists of a mobile phone with an embedded chip that stores an allocated amount of funds already charged to the phone owner's credit card from JCB International [11].

In addition to the transport of people such as in Figure 7, RFID is being used increasingly in the transport and delivery of parcels and postal items. RFID enables improved item tracking during the sorting of mail and delivery processes. More importantly, the technology does not require line of sight to assess an item and to track its location, or to transfer information. This will allow a great number of individual letters or parcels to be routed without physical manipulation.

RFID – Radio that cab fare

Tokyo-area taxi drivers are exploring the possibility of being paid via RFID and mobile phones. Japan-based credit card company JCB International started a trial of the payment system (QUICPay or "Quick and Useful IC Payment") in November 2004.
Selected taxi drivers were given RFID readers, which can read a passenger's mobile phone chip, determine the fund balance remaining, and deduct the requisite amount. All mobile phones used in the trail will be compatible with NTT DoCoMo's mobile wallet handsets. These are equipped with the FeliCa chip from Sony, which uses Near Field Communication (NFC) passive RFID technology.

Figure 7. Taxis, Mobile Phones, and RFID in Tokyo.
From: [17]

Airlines are actively exploring the possibility of integrating RFID in baggage tags, in order to enhance the efficiency of systems employed to track customer baggage. One of the busiest airports in the world, Hong Kong International Airport announced in May 2004 that it would deploy RFID reader infrastructure across its extensive baggage handling facilities [14]. At various nodes within the airport, including baggage carousels, unit load devices (ULDs) and conveyors, reader systems will have the capabilities to read and write to RFID tags that will be applied to passenger luggage. RFID-enabled handheld readers will also be used for handling luggage "on the move."

2. Security and Access Control

RFID technology is increasingly being deployed to control access to restricted areas, and to enhance security in areas such as laboratories, schools, and airports. Many employee identification cards already use RFID technology to allow staff to enter and exit office buildings. The security program of the Canadian Air Transport Authority uses smart cards equipped with RFID first deployed in March 2004. These contactless cards and readers offer physical access control enhanced by biometric authentication to restricted areas.

Educational institutions are also exploring the advantages of RFID for monitoring student populations. In China, in November 2003, RFID deployment began in an

attempt to prevent fraud. China's Ministry of Railways and Ministry of Education were facing problems in authenticating genuine student cards, in particular for the purpose of checking eligibility for travel discounts. Ten million smart labels and microchips were delivered to China's Ministry of Education in 2003. Each chip can hold up to 2 kilobytes of data, and can be read at a distance of 1.5 meters. The chip presently stores the student's identification data and in the future will include all diplomas and degree information. Libraries are also using the chip to facilitate check out and to control the lending of books. Information on the tag is kept secure through the use of cryptography and includes tamper safeguards [16].

In Table 3, the Rikkyo Primary School in Tokyo has taken RFID a step further. In September 2004, the school carried out a trial of active RFID tags in order to monitor the comings and goings of its students in real-time. The system records the exact time a student enters or leaves the campus, and restricts entry to school grounds. Since the tags can be read by scanners from a distance of up to 10 meters, they do not require students to stop at designated checkpoints. The Asia-Pacific region is a leader in this field, but now schools in North America have begun following suit. One example is the Enterprise Charter School in Buffalo, New York which deployed an RFID smart label system from Texas Instruments in 2003. This system, in addition to exercising control over access to the school campus, is also being used to identify and secure assets such as library books and laptop computers. The ID cards enable students and staff to make selected purchases at the cafeteria [18].

RFID - The student's new hallway monitor.
At Rikkyo Primary School in Tokyo, full roll-out of an RFID tracking system is set for April 2005. All students and authorized staff are given active RFD tags, which can be attached to book bags or other personal items. This allows for the real-time monitoring of students, thereby ensuring their safety and thwarting truancy.

The main features of the system are as follows:

1. Individual Recognition via active RFID tags: The system automatically and simultaneously records the comings and goings of multiple individuals passing by the many scanners, at a distance of up to 10 meters.
2. Unobtrusive Monitoring of School Entry or Exit: Due to the 10-meter range, students and teachers need not stop at security checkpoints or specialized gateways.
3. Detection of unauthorized entry – Unauthorized entry is detected by this system through RFID tags and infrared sensors.
4. Privacy and data security – The active RFID tags carry no individually identifying information, but only a number code. Thus, no personal information can be obtained from the tags should be lost or stolen.
5. E-mail notification: The RFID system can send an email notification to parents or guardians when their child enters and leaves the campus.
6. Dedicate Website for Confirmation of School Arrival/Departure: Teachers and staff can verify the arrival and departure of all the children at the school via a dedicated and secure website, which shows both active RFID tag timestamps and security camera imagery. Parents and guardians also have secure access to this site to check information about their children.
7. Urgent E-Mail Network: The system supports an e-mail based urgent contact network feature, for providing important information to the school community on a timely basis. This can be used, for example, in the case of a public safety warning due to accidents or weather-related incidents.

Table 3. Real-Time Tracking of Students at Tokyo's Rikkyo Primary School. From: [18]

3. E-government

Many public sector authorities are considering RFID to make e-government services more flexible, efficient and secure. In the United States, the inclusion of RFID tags on driver's licenses is under debate. The main objective of such tags would be to help thwart fraud. The downside, as many privacy advocates argue, is that such remotely readable tags will make it easier for government agencies to spy on citizens and increase the possibility of identity theft. The Commonwealth of Virginia is one of the first states

to consider the use of RFID in drivers' licenses. In February 2005, the United States House of Representatives approved a measure that would compel states to design their driver's licenses by 2008 to comply with federal antiterrorist standards [15].

RFID enables the so-called "Internet of things," which may be further extended to the tracking of human beings. The United States' Food and Drug Administration has already approved implantable RFID chips for people. The concern among ordinary citizens and privacy advocates concerning this development is undeniable as hoax stories such as a U.S government plan to implant all homeless people with RFID tags have been widely circulated over the Internet.

In Europe, there has been increasing press coverage since 2001 on the possibility of embedding RFID on Euro bank notes, in order to thwart counterfeit, fraud, and money laundering. The European Central Bank has been in discussion with various technology partners such as Philips Semiconductors, Infineon, and Hitachi on projects to tag European currency.

4. Defense and Security

RFID offers significant potential for governments wishing to fortify their national defense and security systems, particularly in a climate plagued with increased international terrorism. Border crossings offer a good example. The border between the special administrative region of Hong Kong and Schenzhen, China is highly regulated and is a case in point since 2002. Schenzhen authorities have installed an RFID system to facilitate the flow of low-risk traffic and goods across that border and to thwart smuggling [14].

5. Sports and Leisure

In the sporting world, RFID tags have been used in marathons to track runners [see Figure 8], allowing both participants and spectators to benefit from the combination of mobile SMS and RFID. RFID technology has been used to determine with remarkable accuracy the winner in an Indy 500 car race by tracking cars as they pass the finish line.

Hands-free access systems using RFID for ski lifts have been introduced since the last 1990s. In 1999, Texas Instruments together with the Austrian company TeamAxess deployed an RFID system for access to ski lifts and slopes in Europe [14]. Remote-operated gates equipped with readers can detect a valid ski pass and open automatically, leading to shorter line-ups and more efficient customer processing. The credit-card sized RFID-enabled ski pass can easily fit into a jacket pocket, and is scanned in place, preventing the need for manipulation. The passes can also be used to locate skiers in case of injuries or for the location of children.

RFID can also assist in preventing theft of property, particularly in relation to travel or leisure activities. In Germany, Philips Semiconductors introduced an RFID labeling system to protect recreational boats from theft by providing secure electronic identification [15]. In the past, boats were simply identified by painting numbers on them. This system of identification suffered the considerable disadvantage of fraudulent removal or modification. Since RFID tags allow the identity of a boat to be determined remotely, German authorities can check the status of a boat against their databases of stolen and registered boats, without the need for a search warrant. The RFID labels are thin and waterproof, and can be read at a distance of up to 60 centimeters, even through materials such as wood or fiberglass. Plans to extend the current system to other forms of high value property such as trailers, caravans and bicycles are being actively considered.

In the travel and hospitality industries, RFID tags are enhancing and facilitating customer service. Manchester City Football Club in the United Kingdom was the first football club in Europe to adopt RFID, giving fans ticket-less access to football grounds and significantly reducing the time it takes spectators to enter the grounds [11].

Marathon organizers in such cities as Boston, London, New York, Berlin, Los Angeles, and Capetown are bringing high-tech communications to participants as they run the course.

For example, all of the official entrants in the 2004 Boston Marathon were issued with the "ChampionChip", a small token that is either tied onto the runner's shoe or attached to a wheelchair. These chips time the runners at various points throughout the race, including the starting line. As a runner crosses stationary mats located throughout the race, his/her time is recorded. The chips contain RFID tags that transmit the runner's time at the checkpoints to databases operated by the Boston Athletic Association and its technology partners (Hewlett-Packard and Verizon Wireless).
Some 33,000 runners competed in the London marathon on 18 April.

Figure 8. RFID Tracks Runners in Marathon.
From: [19]

6. Anti-Counterfeiting

Counterfeiting is a huge threat to global businesses and concerns all kind of products and companies including pharmaceutical industry, automotive industry and their suppliers, luxury goods, media, food and beverage, banknotes, and passports. The pharmaceutical industry is now testing RFID technologies to track and trace their product. The FDA Anti-Counterfeiting Task Force has strongly suggested the use of RFID to safeguard against pharmaceutical counterfeiting. According to a report from the META Group titled "RFID in Pharmaceutical Industry," RFID adoption in the pharmaceutical industry may surpass retail adoption within the next 24 months. Tracking pharmaceutical product is a vital safeguard measure since it is estimated that more than

ten percent of pharmaceuticals distributed worldwide are fraudulent [30]. In one trial deployment, medicine bottles are being fitted with RFID tags in order to detect fake drugs moving through the supply chain. Other pharmaceutical deployments include recall management and return management – the FDA Office of Compliance reported 1,230 drug recalls between 1997 and 2002, or an average of 3.9 recalls per week, inventory management, product authentication, pedigree management, and sample management. According to an ARC Advisory Report titled "RFID Systems in the Manufacturing Supply Chain," over 12 billion pharmaceutical units are candidates for RFID tagging. The same study predicted that most pharmaceuticals will be tagged by 2007 [31].

The EPC Network allows the tracking and tracing of products that allows companies to retrieve and view a product's history. Additionally, RFID technology allows the products to authenticate themselves to the user through the use of an authentication server employed in the EPC network that can be established at the user's designated location. Sun Microsystems recently released an RFID package focused on helping pharmaceutical companies track and authenticate drugs in their efforts to combat counterfeiting, product piracy and smuggling [24].

D. IMPLEMENTATION LEADERS IN HEALTHCARE INDUSTRY

The use of RFID has already begun in several hospitals across the country. Many companies are already focusing their time and energy towards the realization of this goal. These companies include the following:

1. Agility Healthcare Solutions (AgileTrac)

Agility uses RFID technology to enable tracking and identification of mobile assets including medical equipment, surgical instruments, supplies and pharmaceuticals. RFID has been used in several industries for many years, but Agility is the first to offer RFID-enabled resource and workflow management solutions designed to optimize asset utilization, reduce operating costs and improve care quality for the healthcare industry [20].

RFID uses tiny tags affixed to medical equipment, containers and supplies to transmit accurate, real-time information to resource and workflow management applications. Similar to a bar code, RFID encodes data into a carrier that allows the data to be read from a reader. The RFID tag responds to signals received from a reader. In most cases a tag is associated with the item to which it is attached and provides identification for that item when the tag is read.

Unlike a bar code, RFID encodes data into a carrier for wireless data transfer. In the healthcare setting, most bar code solutions require a person to scan a bar code to capture data. RFID offers the tremendous advantage of automated scanning, eliminating the need for this manual scanning activity. RFID is superior to other automated data capture technologies, such as infrared (IR) technology [21]. While IR minimizes the manual scanning of bar codes, it also requires line-of-sight to gather data.

Through a five-year, $3.9 million contract deal, Agility Healthcare Solutions designed and implemented an RFID system at three Virginia hospitals operated by Bon Secours Richmond Health System. This system tracks the mobile medical equipment around the hospitals. Agility also is responsible for the operation and the management of the RFID system. According to Agility, Bon Secours will get a return on its investment within the first full year of operations, by deploying its “AgileTrac” program [28].

Exact location of more than ten thousand tagged equipment items will be tracked on a real-time basis using the AgileTrac RFID system using the configuration in Figure 9. The tags will operate at 303 MHz. By transmitting at 303 MHz, the readers will operate well outside the frequencies used by other medical or scientific telemetry systems found in hospitals. Using this frequency also gives the readers a long-range capability. Hundreds of readers deployed across the three hospitals, have built-in 802.11b capabilities to connect to a wireless Local Area Network (LAN). This allows the readers to communicate with the central inventory management system also hosted by Agility. Using wireless LAN also allows the hospitals to reconfigure the network as the need arises.

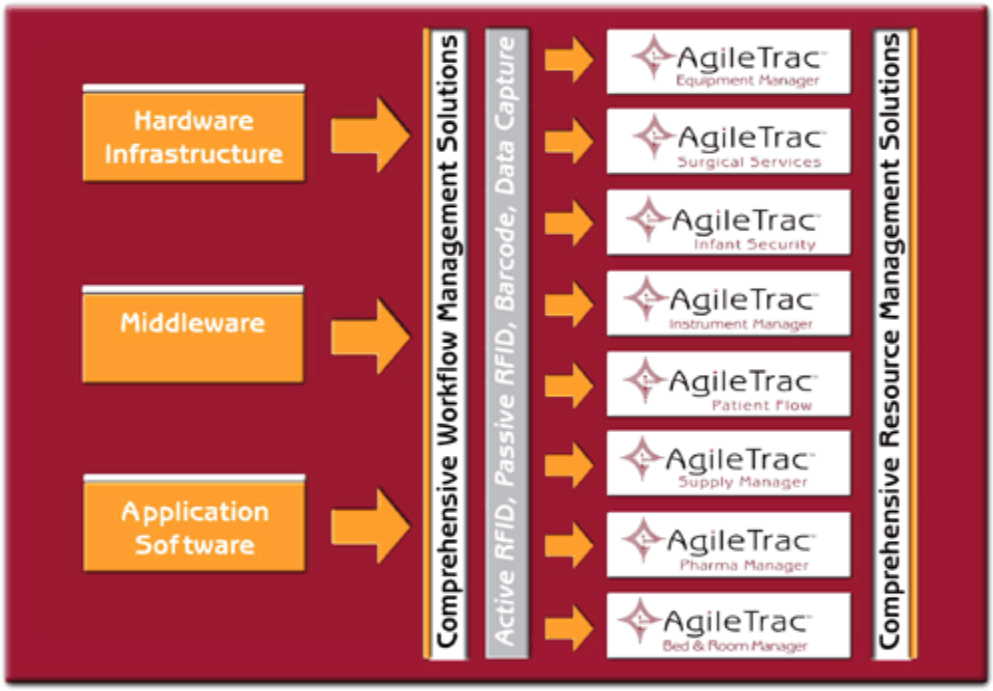


Figure 9. Agility "AgileTrac" Configuration.
From: [20]

2. Exavera Technologies – eShepherd

Exavera Technologies released its eShephered system that combines RFID and Wi-FI technology to track people inside a hospital [21]. Exavera claimed that this system can bring enormous savings to hospitals and healthcare centers. Exavera also claimed that an average-sized hospital with 250 beds can save nearly four million dollars a year for an investment of just $400,000 that covers the equipment and installation costs. These savings come mainly by ensuring that patients receive correct treatments and medications.

Some estimates showed that as many as 98,000 people die in the United States each year because of medical errors. In cases where a patient does not die from an error, the mishap ends up costing the hospital an average of $4,700 per Adverse Drug Event (ADE). Many of those errors could be avoided by using the RFID technology. Exavera believed its technology delivers an integrated hardware and software platform that all hospital departments can use to communicate.

The eShepherd system combines RFID with Wi-Fi and Voice Over Internet telephony (VoIP) to deliver a single system to track patients, staff, and hospital assets.

The unit can connect to the hospital's LAN through a central router, and it can handle telephone calls over the wireless network. The unit also includes an RFID reader to read RFID tags placed on patient bracelets, staff identification badges, and hospital equipment. Exavera uses RFID tags operating at either 433 MHz or 915 MHz for the United States market and 869 MHz for the European market, as well as 2.4 GHz. Exavera devices have read ranges up to 45 feet with the passive tags worn by patients and up to 90 feet with the active tags that would be worn by staff.

Nurses and doctors wearing RFID-tagged badges will also carry handheld devices that will allow access to a patient's medical record whenever they detect proximity to a patient. The eShepherd system will help ensure that patients get the appropriate medical care. In addition to reducing medical errors, the system will also improve various process efficiencies. By carrying handheld devices, doctors will be able to view any patient's complete medical record whenever they need to, instead of having to repeatedly walk to a central filing area to retrieve the information. The system can also be used to locate equipment, staff and patients on a real-time basis. The eShephered system is currently used in two New England hospitals. One hospital has a twenty-five bed capacity and the other has a ninety-nine bed capacity. The twenty-five bed facility deployed the RFID system in an eight thousand square foot wing of the hospital but required only two Wi-Fi router transceivers.

Exavera's systems also provide the mechanism to meet security and privacy regulations set by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the requirements regarding positive patient identification established by the Joint Commission on Accreditation of Health Care Organizations (JCAHO).

3. University of Memphis Fedex Center

Memphis-based systems integrator American Project Services (APS) teamed up with the University of Memphis' Fedex Center for Supply Chain Management and the Shelby County Regional Medical Center's Trauma Emergency Department to deploy an RFID network [22]. The ultimate goal of the project was to track the time taken by patients at each location in the trauma center. This information was intended to be

provided to the center which will then use the data to streamline its service and improve patients' experience.

The first phase of the project was to validate the RFID technology and the results the system generated. RFID tags were attached to patients as they entered the facility. The technology worked faultlessly, reporting with one hundred percent accuracy. By automating the collection of data, the APS trial also showed that RFID technology could track patients without altering the study's results. This was in contrast to the findings when barcodes or other manual data entry systems were used in collecting data. Using barcodes or other manual data entry systems distorts the data because the people involved in entering the data are constantly reminded that they are being monitored. Research has shown that people perform differently when they know they are being watched.

The trial used tags and readers from Alien Technology and operated at 2.45 GHz. The two-inch by three-fourths inch tags included a battery to enable a longer reading range. The read range was up to thirty meters compared with the three meter capability with the passive tags. The tag comes with a twelve-byte unique identification number that was used in the trial. Twenty-five RFID readers were deployed throughout the approximately 250,000 square foot facility which included the X-Ray rooms, two CAT scan rooms, two Intensive Care Units (ICU), an operating room, and several general areas. During the trial, an RFID tag was attached to an ankle of arriving patients as soon as they entered the center. The tag's unique identification number was tracked without recording any information about the patient or patient's injury.

4. Maxell – Test Tubes

At the Automation 2005 show held in San Jose, California, electronics company Maxell showcased an RFID system to track test tubes in a laboratory. Working with Japanese companies Kobe Bio Robotix and Tsubakimoto Chain, Maxell aims for the system to replace those of bar codes used commonly today. Improvements of the RFID system include the ability to scan a shelf of RFID-tagged tubes instantly and rewrite features that allow information stored on each tag to be updated and modified over time.

Maxell Corporation conducted research on the feasibility of attaching its RFID "coil-on-chip" tags to the base of plastic test tubes. The company developed an RFID reader that will read and write to a tray-full of tagged tubes. Looking into the future, Maxell had the vision of a large market for its system for use in the medical diagnostics and pharmaceutical industry.

Maxell's Coil-on-Chip tag measured 2.5 square millimeters and operated at 13.56 MHz which only allows a very small read-write range [23]. As such, Maxell designed the system so that a tray of test tubes can be placed on top of the reader keeping the distance between the reader and the tags within acceptable limits. The antennae are mounted directly onto the surface of the silicon chip. Figure 10 shows the tags embedded to the bottom of the test tubes. These tags can store between 128 bytes to four kilobytes of data.

Figure 10. Embedded RFID Chip Helps Track Samples in Test Tubes.
From: [23]

THIS PAGE INTENTIONALLY LEFT BLANK

III. REQUIREMENTS FOR RADIO FREQUENCY IDENTIFICATION IMPLEMENTATION

A. STANDARDS

Radio Frequency Identification technology represents more than a simple change to the methods by which products are identified. It represents a major paradigm shift in automatic identification. As such, it will significantly impact operations in business applications ranging from supply chain management to healthcare environment.

The key to worldwide interoperability of the Radio Frequency Identification technology is consistent standards [34]. While standards often seem to slow development of new functionalities, they actually integrate good ideas from many sources and accelerate the acceptance of increased functionality. As their use in a field matures, standards also help ensure the existing infrastructure is ready for the new uses. Recent standards recommendations have set the stage for rapid deployment of RFID technology.

To understand the impact of RFID standards to the business environment, revisiting the use of standards in the barcode system could be used. To this day, a scanner has to be configured to read certain types of bar codes. Many companies have their own bar code specification requirement. While some of these unique requirements may remain in the RFID implementation, the industry has learned a lot with the evolution of the barcode standards that can be used to make the RFID implementation more efficient.

RFID compliance standards provide the following benefits:

- Facilitate communication
- Promote collaboration
- Encourage global competition
- Support software interoperability
- Reduce loss
- Accelerate acceptance

Two vendors agreeing to adopt a similar communication protocol may be convenient on a short term basis, but may become unmanageable on a larger scale. Standards can only be truly effective if they are universally adopted and applied.

Beyond facilitating communication between partners, RFID standards support interoperability between the products of one vendor with the products of all other vendors who conform to the standard. At the same time, standards allow global interoperability by ensuring that all vendors collaborate on solutions. Therefore, RFID standards encourage global competition and broaden the markets.

The ability of RFID standards to broaden global communication also encourages software interoperability. In return, RFID facilitates further application development and provides a development platform for complementary products. The adoption of universal standards provides enterprises with the ability to create fully integrated solutions that touch every aspect of their enterprise. Consequently, RFID standards have the additional benefit of reducing prices for the end users.

Aside from the communication and development implications of standards, they can also help accelerate RFID acceptance. The universal acceptance of consistent RFID standards helps increase customers' confidence in the long-term viability of the RFID processes.

Standards are designed to ensure that the RFID reader and tag communications layers are able to:

- Recognize and identify one or more RFID tags within the readers' field
- Manage the anti-collision algorithm that allows communications with several RFID tags within the same field.
- Determine the presentation of the data
- Determine the tag memory size
- Read all or part of the data stored in the tag
- Send data to the RFID tag to exchange or extend the data stored
- Manage the data transfer and the session
- Maintain integrity of the data read/written

- Provide authorization for reading or writing
- Protect stored data
- Provide security during data transfer

Early adoption in RFID business processes was limited to the pallet level in the supply chain management arena. As such, standards were established to meet certain pallet level data requirements in addition to the communication requirements for RFID tags. These data requirements included:

- Generic – allow anything to be identified/tracked or traced
- Internationally compatible – supported by recognized standards organizations
- Time and cost reduction – reduce errors by helping integrate logistics operations internally and externally
- Data rich – supports a wide range of information for all parties through the use of application identifiers
- Connected – provide a link between the physical flow of goods and the electronic information flow

1. Variations of Compliance Standards

Most of the attention for RFID compliance standardization are focused on the Electronic Product Code (EPC) and International Standards Organization (ISO) who are expected to come together in the near future to provide a single global standard.

a. Electronic Product Code (EPC)

The prevailing compliance standard is the Auto-ID Center's Electronic Product Code (EPC). The organization overseeing the EPC model is EPCglobal Incorporation which is a joint venture of the Uniform Code Council and European Archival Network (EAN) International.

The EPC Numbering System uniquely identifies objects and facilitates tracking throughout the product's life cycle. This makes it similar to the Universal Product Code with the main exception that EPC was primarily designed to be efficiently referenced on networks. To achieve a global tracking system that involves connections

between several companies and information systems, standards such as EPC are important.

The EPC is the fundamental identifier of assets in the EPC network. It basically contains information about:

- The manufacturer of the tagged object
- The product class or the nature of the tagged object
- The actual (unique) item. This serial number is the main benefit over classical barcodes where two cartons of orange juice, from the same brand, of the exact same kind, will have the same code.

Each of the above information is encoded in a separate field which makes it easy to extract only part of the data. EPCs are often represented as Uniform Resource Identifiers (URI) in order to be used on large networks and to be easily manipulated and exchanged by software applications. This enables the handling of EPCs in a tag-level independent manner and decouples the application logic from the way of obtaining the EPC. The URI contains the EPC fields required to distinguish an object from another. A pure entity representation of the EPC on Figure 11 is:

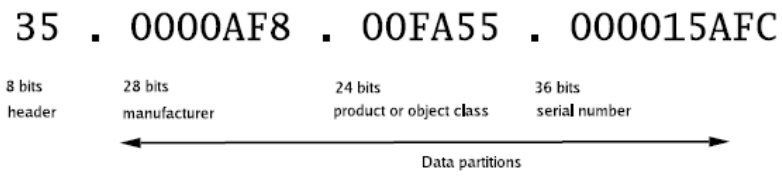


Figure 11. Hexadecimal Representation of an EPC. From: [24]

The first field corresponds to the EPC encoding schema, the second to the company prefix, the third to the asset type, and the last to the unique serial number.

Current EPC standards use a two-level classification. The first classification (Class) represents the tag technology and indicates how data is programmed

into the tag. The second classification (Generation) refers to the physical layer of the device and defines the amount of data that can be written. Current EPC standards are defined as follows:

- EPC UHF Class 0: Read only tag that supports 56 bits of data and operates in the 860-930 MHz frequency range
- EPC UHF Class 1: Write Once Read Many (WORM) technology. In the first generation, the Class 1 Generation standard supported 96 bits of data and operated in the 860-930 MHz range.
- EPC UHF Generation 2 Foundation Protocol: Sufficient data storage of up to two kilobits WORM and two kilobits Read/Write has led to wide acceptance in the marketplace. It is targeted to meet user requirements on a global basis and also projected to increase the data storage capacity to 1028 bits in the Class 2 standard to be able to support the Department of Defense requirements for identifying goods in the absence of a database environment.

b. International Standards Organization (ISO)

The International Standards Organization (ISO) is the most respected worldwide standards organization. The standards that the ISO is working on can be used anywhere in the world to specify how RFID can be used for a variety of applications.

RFID tags that comply with ISO specifications can carry information that follows the structure established in the EPC specifications. Users will be able to utilize the EPC numbering system with the interoperability and protection of open international standards.

- ISO 18000 parts 1, 2, 3 and 4 cover the generic parameters for the air interfaces at all major frequencies as well as specific air interfaces for tags operating at 135 KHz, 13.56 MHz, and 2.45 GHz.
- ISO 18000 part 6 covers the air interface for RFID tags operating at Ultra High Frequency (UHF) in 860-930 MHz range.

- Draft ISO standards 17363-17368 cover different types of logistics containers and packaging in addition to individual items. Draft ISO 18185 covers electronic container seals for logistics security.

B. USER REQUIREMENTS

The promise of increased functionality in RFID systems created in compliance with the established standards created a foundation for the new era of RFID implementation. Momentum and mandates quickly established guidelines for RFID systems used by global organizations and their trading partners. Using the established standards, a foundation for RFID implementation was created on which to build interoperable RFID products and systems that will improve deployment and management of various operations around the world. Despite the creation of such standards and the realization that many hospitals have similar information needs and comparable business practices as other hospitals throughout the nation, it cannot be expected that the usage environment for such information will be the same. Since any implementation of RFID technology cannot provide exactly the same performance at any two facilities, it is important to recognize some of the common key user requirements for RFID implementation to provide the information needed to define the performance expected in relation to the environment in which the system is deployed.

1. Speed

The ability to read RFID tags quickly and simultaneously is fundamental to many of the application benefits the technology can provide. Efficient identification, distribution and inventory management requires the ability to identify and differentiate patients, staffs, and equipment moving around in hospital environment without having to slow down the normal processes normally carried out in providing medical care. Despite the lack of a firm or minimum speed specification within the standard, a successful RFID implementation providing an ideal reading speed will depend on many variables including power output, tag density, and the radio frequency environment.

A new generation of RFID tags and readers support the “group select” feature that is very important for providing high-speed reading and identification. Group select provides the capability for RFID readers to be set to seek and read select groups of tags

based on the data structure and to ignore others in the field [29]. Using this capability, readers can be set to ignore hospital visitor tags and record patient tags if the need to track down patients arises. This feature reduces the amount of data the system must process and increases the reading rate for any identified tag of choice.

Since user will always need to be assured that all tags will be identified as they pass through the read field, it is equally important for the reads to be correct as it is to be fast. Reliable systems make efficient use of their speed and identification protocols to constantly monitor the read field to ensure that tags that enter a designated area late are still identified.

2. Bandwidth Efficiency

Wireless bandwidth is limited, highly regulated and must be managed carefully. There is much more to bandwidth management than selecting a frequency. Other technical factors such as signal modulation, power output and the presence and density of other RF devices in the environment must all be accounted for. Despite the fact that standards and specifications address most of these variables that affect the use the technology and bandwidth utilization, users are expected to make some important decisions in some situations.

Most RFID products can be used throughout the world without licensing restrictions and will provide the range, speed and other performance needed to meet the application requirements spelled out by users in correlation to their respective bandwidth limitations.

3. Reliability

Not every application requires the high speed reading and advanced bandwidth management but every user needs to be sure that all tagged items are identified accurately [28]. EPC numbers follow a defined data format which makes it possible for systems to verify data read from and written to the tag. The standard shifts data checking from the reader to the interface which enables faster execution. This also adds protection against receiving false positive readings that are also known as ghost tags. These ghost tags are

recorded when the reader picks up portions of data from different tags and interprets them as the identification of a single, non-existent tag.

Current RFID devices will also perform more reliable in a wider range of operating temperatures. Traditionally, synchronizing tag and reader timing could be accomplished in a tag manufacturing procedure that added expense and limited the temperature range in which the tag could function.

Device reliability can take on added importance in RFID systems as they tend to feature more unattended operations. A worker with a handheld bar code reader can keep trying to scan a symbol until he or she gets a confirmation beep. Users can also call attention to equipment that may need service or fails altogether. These safeguards are not available for an unattended, portal, or similar systems. Remote monitoring, diagnostic and notification capabilities should be built into the equipment itself so the system can provide the performance, uptime, and reliability that RFID operations require.

4. Range

User requirements dictate the range required from every RFID system. In a supply chain environment, companies may only need to capture pallet tag information from a few feet away with handheld readers before shipping pallets to a customer. At the next stop, tagged cases might be stacked high on warehouse shelves where much longer read range is required. In the same way as speed, there is no specified range requirement because of the many variables that affect range which include interference, reader power output, the amount of time the reader can continuously transmit, and reader density. Current specifications enable range to satisfy user-defined application requirements.

5. Security

Current RFID tags are protected against tampering. The standard protocol includes encryption and requires the tag and reader to create a secure link before data is transmitted which makes it very difficult to alter the communication link. The standard also provides the ability to disable the tags in the field so their data can never be accessed which is a requirement in the retail and consumer goods industries to allay customer

privacy concerns. It also has authentication requirements to prevent unauthorized and accidental disablement of tags.

Additional security features can also be implemented to create differentiation among the RFID devices. Cloaking enables tags to be set so they will only communicate with authenticated readers. Readers must provide a password before the tag will respond with any communication. Passwords may also be required to write to tags or disable them.

New applications such as lot code or expiration date tracking will take advantage of the data content flexibility that improved tags allow. It is important to note that supplemental data does not automatically get the same protection as the originally encoded tag. As a result, users must take steps to secure and validate data. Security is required to ensure additional data written to tags is protected. Supplemental tag data also can be password protected so it is available only to select users.

6. Cost

A leading motivation for development of the EPC system was to create RFID technology that was cost effective for use in supply chain operations. Development efforts focused on creating specifications to enable the production of low-cost chipsets and equipment. Initial user experience with the technology revealed that low-cost designs had fatal limitations when used in real-world operations. Reliability, data security, and range were among those limitations identified [12]. The user community provided clear directions to the standards committee to improve tag and reader functionality. Current RFID tags and readers strike a balance between cost and functionality that should lead to the development of cost-effective products that satisfy real-world application requirements.

C. CHALLENGES

1. Introduction

Radio Frequency Identification generates tremendous excitement among business leaders as this technology undoubtedly holds promise to organizations with the potential for greater efficiency, control and accuracy over their business practices. Similar to the

evolution of other emerging technologies, several challenges must be overcome for RFID technology to mature to its full potential. In the case of RFID, some of these challenges include the following:

a. Standards for RFID Systems

The use of standards in RFID technology, applications development, and deployment is a multi-tiered issue. For example, standards are needed to specify performance of tags (whether passive or active) to ensure that tags meet intended designs such as single-write/multi-read tags, multi-write/multi-read, or for potentially sensitive applications requiring a built-in disable function as in single-write/single-read tags. Standards also cover the air-interface operational requirements such as the parameters for interaction between a tag and the tag reader including transmission and receiving frequencies, algorithms by which the tag reader can communicate with the tag, and when the tags would respond to a reader query in the case of active tags. Another set of standards is required for the software that supports the readers and the tags, and for the data obtained from the tags. Standards would also cover systems for coding information contained in the RFID tags, for handling the estimated terabytes of data generated from the information contained in the tags, and for ensuring the adequate protection of data for both security and privacy concerns.

In addition to these initiatives, activities are also underway in private sector organizations such as EPCglobal Incorporated, the global consortium that manages the UPC information in bar codes. EPCglobal has developed a series of specifications that cover issues such as physical placement of the tag, tag-coding structure, tag data specification, and air interface. EPCglobal has recently ratified a Generation 2 specification that it claims would allow for global interoperability of systems built to this specification [34].

The AutoID Labs have also developed a standard (Savant) for defining how the middleware system will organize data gathered by a RFID reader and make the data available for an enterprise application [35]. In addition, many vendors and RFID systems developers and implementers continue to develop protocols and specifications to meet the unique needs of their consumers.

Standards development activities covering the issues raised above are also underway in different discussions around the world. Globally, there are approximately 120 different protocols currently in use as tag standards. In recognition of the diversity of protocols, several standards harmonization initiatives are currently underway. For example, development of RFID standards is underway in organizations such as the International Organization for Standardization (ISO)/International Electrotechnical Committee (IEC). A working group under the joint ISO/IEC Committee (ISO/IEC/JTC1/SC31/WG4) has developed the 18000 series of standards (18000-1 through 18000-7), to address issues such as the "Generic Parameters for the Air Interface for Globally Accepted Frequencies" and the "Parameters for Air Interface Communications" at different operating frequencies [34]. The standards do not include several issues including data content, structure, and physical implementation of the tags and readers. Two other subcommittees and their working groups (ISO/IEC/JTC1/SC31WG2 and ISO TC104/SC4/WG2) are developing standards on data structure and standards relative to Automatic Equipment Identification and intelligent container seals.

A major concern with the multitude of RFID standards development activities is the possibility that standards development in these bodies may not be coordinated and could result in multiple or conflicting standards. Multiple and conflicting standards may also hinder technology development and deployment and reduce the anticipated benefits of RFID. The existence of multiple standards forces the technology application developer to choose between standards and develop applications that might work under one standard and not the other.

Another concern is the inappropriate use of standards by countries or organizations that might look to protect internal markets and mandate certain standards for reasons other than technical merit or interoperability. Challenges may also arise from standards established to meet immediate requirements, such as reduced time to market, and short-term economical gains that do not have the flexibility to incorporate future technological advances and developments. Other limitations to harmonizing standards may arise when organizations develop standards based solely upon the infrastructure presently available. For example, RFID standards in a country using the high frequency

(HF) range for RFID operations, may be very different from those required in a trading partner country that uses the ultra high frequency range (UHF) for its RFID operations.

The successful development of RFID standards and deployment of the technology relies heavily on the cooperation and collaboration of the standards developers, whether in an international or a domestic setting, to ensure that RFID standards are based on technical merit and support interoperability.

b. Immature Technology

It is important to remember that RFID is still an emerging technology. While it is also true that there is nothing new about the technology behind RFID since radio frequency devices and their transmission of data to computer systems such as clothing tags and EZ-Pass cards have been in operations for years. The massive unified application and lending adoption of RFID in manufacturing, retail and supply chain management must be perceived as a unique industry evolution separate of other implementations.

A basic analogy can be made with Extensible Markup Language (XML). Standard Generalized Markup Language (SGML) was certainly present and in use to an extent by varied industries, but the collaborative effort of XML definition, education, and adoption by academia, government, consortium and private industry was a breathtaking process in its scope [36].

c. Changing Specifications

Due to the immaturity of the RFID technology, fluidity in the specification can be expected. This fact should not be considered critical of any consortium or standards committee. On the contrary, many individuals and groups are working diligently to refine and solidify specifications for RFID, regardless of whether they are working on the tags, readers, or the radio frequency transmission itself. Yet, with such a growing interest in radio frequency tag implementation, the dynamic nature and flexibility of RFID is the very aspect that slows specification advancement [43].

d. Product Quality

RFID tags and readers are still maturing in their consistency, stability, and durability. This technology is not typically found in a clean-room environment. Tags must be rugged but inconspicuous on products and durable and lasting but inexpensive.

These are difficult goals to achieve for RFID tag manufacturers so early in a technology life-cycle. Cheap, lasting, inexpensive circuitry is a lofty goal for manufacturers who are still in the expensive part of the research and development curve.

e. Hardware Inconsistencies

RFID tag readers are farther along in maturity due to the inability of hardware vendors to borrow device traits from UPC and other existing readers [42]. Manufacturers also believe that the interface and complexity of the readers add to inconsistency problems during deployment. UPC readers benefit from singular tag reads, line-of-sight, and other situational features. The necessity of RFID readers to read multiple tags and advanced features such as tag data analysis and tag data manipulation introduce device complexity with regard the interface, device health, and troubleshooting.

f. Situational Read Rates

The flexibility of RFID readers to read data from tags is certainly one of the most touted features of RFID. Even with this advantage, readers are still prone to tag reading failures. Without close direct access to the tag, an RFID reader must transmit a signal from a distance, even through solid materials. Certain materials and metals create RFID transmission difficulty. With accurate accounting accuracy a necessity for businesses, RFID must overcome these obstacles through technology, implementation, and business education.

g. Conflicts with Other Transmissions

Similar to other devices using signals for communication, other competing signals present in the same environment can impact the strength of RFID transmission. There are many devices in the healthcare environment that emit, either intentionally or unintentionally, waves of varying frequency. RFID implementations must account for other devices, so that other instruments do not hinder RFID use while ensuring that RFID does not hinder the functionalities of other instruments.

h. Competing Standards for Transmission Protocols

The actual RFID protocol and frequency has larger implications for industry adoption. Other technology standards that have had substantial interest and appeal, such as CDs and DVDs, have had fragmentation and competing standards, created and backed by the leaders of the industry [24]. Intellectual property, patents,

intimate technical knowledge and publicity are all reasons for organizations to win such standards battles. It will be interesting to observe how RFID will mature in the definition and implementation with respect to the current and future standards.

i. Business Process Aspect

If hospitals are going to invest in RFID implementation, their stakeholders will expect benefits and results. While the efficiencies gained by RFID alone are worthwhile, hospitals truly benefit when this aspect is combined with business processes such as supply chain management, work flow and data intelligence and analysis. As was expected by many industry experts and is already showing to be the case, RFID implementations are being executed by organizations in conjunction with modifications and advancements in their business practices.

j. Data Distribution

RFID tags allow for data to be stored and transmitted to readers. This capacity is only beneficial if that data is later used by the organization. Wasted, ignored and neglected data stored on RFID tags keeps businesses from maximizing the potential of RFID technology. RFID implementations should always consider the data to be stored and its utility during the planning stage. True utility is seen in this data storage medium when it flows to an organization's ERP system, their mail systems, their work-flow engines, inventory databases, reporting elements and B2B systems [27].

k. Training and Education

With so much consideration and concern about the technical elements of RFID, businesses can easily forget about the human element of the technology. Employees of all levels should be informed and trained about the merits and aspects of RFID. The more education is done at an organization, the higher the likelihood that those employees will properly use, appreciate, and intelligently adapt RFID to their environment.

IV. BENEFITS FROM RADIO FREQUENCY IDENTIFICATION IMPLEMENTATION

A. INTRODUCTION

There is always a crowd of things and people going around in a hospital that need to be tracked. There are doctors, nurses, patients, and visitors who need to be kept track of in times of emergencies. Additionally, assets such as equipment and other devices need to be tracked to prevent them from getting stolen. Medications also need to be tracked to provide patient safety in ensuring medicines are given to the right patient, in the right amount, at the right time, and in the right location.

1. People

Various hospital personnel that can be tagged and tracked using RFID include:

a. Doctors

The need to track doctors' location can be explained using the following scenario: An emergency occurs in the hospital and all the doctors are elsewhere in the hospital. The nurse pages the doctor about the emergency. The doctor responds after some time, but by the time he arrives, it is too late to administer any life-saving measure. This is exactly the scenario that needs to be avoided. If the location of the doctors can be tracked on a real time basis, a better arrangement and distribution solution can be implemented to ensure the availability of at least one doctor in every area of the hospital to take care of such emergencies. Doctors can wear bracelets or badges containing RFID tags.

b. Nurses

There is usually far more nurses in a hospital than doctors. For this reason, even distribution is seldom a problem in their case. Still, it is equally important to keep track of the nurses. For example, keeping track of close contact with patients having infectious diseases is of utmost importance for the health of the hospital staff. In Singapore and other Southeast Asian countries, RFID became an important tool in fighting against Severe Acute Respiratory Syndrome (SARS). All hospital staff was tracked for close contact with a SARS patient and then were appropriately treated [25]. Additionally, in the case of medical error, it may be important to track the nurses who

were responsible for giving the medication to the patients. Like doctors, the nurses can wear the tags as bracelets or badges.

c. Patients

Each year, between 44,000 and 98,000 patients die because of medical errors [26]. Currently, only three to four percent of the approximately 64,000 hospitals in the United States have an integrated Hospital Information System (HIS) to manage patients' records and care. In addition, sixty percent of those hospitals with HIS are using bar code technology to ensure patients receive the right treatment [21]. The number of fatalities can be significantly reduced by incorporating RFID in the hospitals for increasing the accuracy of reads. If every patient is required to wear an RFID tag similar to the tags shown in Figure 12, all his/her records can be placed in a central computer and can be accessed by all authorized doctors and nurses on their handheld computers simply by scanning the tags he/she is wearing [see Figure 13]. Every life saved will more than cover the cost of implementing the RFID systems.

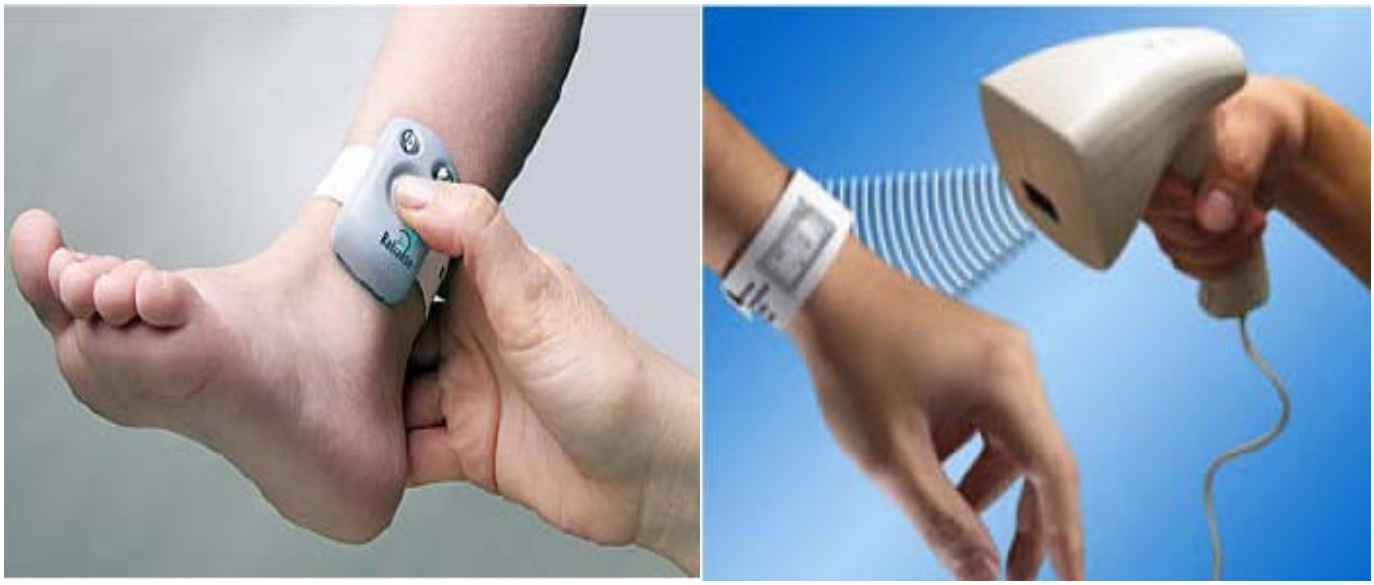


Figure 12. RFID Tags Attached to Outpatients.
From: [26]

RFID for tracking proves beneficial in tracking restraint patients suffering from mental breakdown to ensure tracking in the event they get loose from restraint and

start to wander off. RFID tracking is also an ideal mechanism for tracking personnel under police custody that are taken to hospitals for medical reasons to determine their location in case they gain the opportunity to escape their escorts and present undue potential risks to other patients.

Figure 13. Inpatient RFID Tracking.
From: [27]

d. Newborn Babies

Most hospitals employ mechanisms to ensure that newborn babies are "tagged" with a device that would trigger an alarm if a newborn was taken away from a designated area without proper authorization. Using RFID, newborn babies and their mothers are identified using RFID-laden bracelets that would have the same code written on both tags. In most situations, babies wear locked RFID tags on their ankles. With this system in place, hospitals are assured that if a mother deliberately or mistakenly picked up a baby that was not hers, an alarm will be triggered to alert the staff. Additionally, this helps prevent any unauthorized individual to be in the maternity ward from picking up a baby and holding him/her without a maternity nurse or the mother's approval. Authorized maternity ward nurses on shift carry an RFID tag that corresponds with all tags, preventing false alarms to be triggered.

e. Visitors

When there are patients in the hospital, there will always be visitors to see them. Most of the time, these visitors might wander away into the restricted areas of the hospital. Putting an RFID tag on every visitor can help eliminate this problem by linking them to a unique patient. An alert will be triggered each time the visitor wanders away from close proximity of the patient they are there to see. The visitors can wear badges or bracelets containing RFID tags as shown in Figure 14.

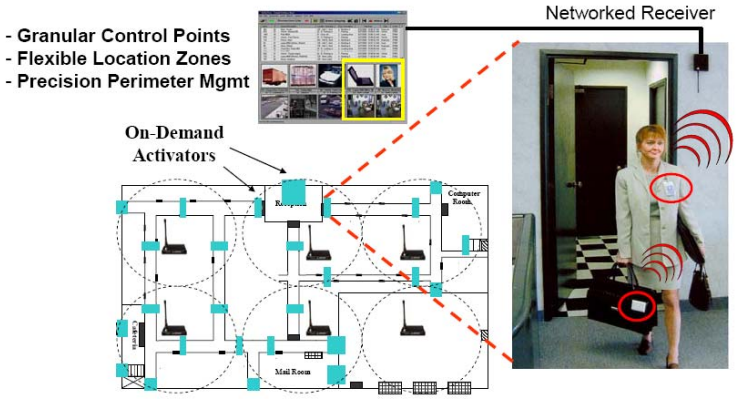


Figure 14. RFID Tracking of Hospital Visitors.
From: [28]

2. Equipment

Medical equipment available for tagging and tracking include:

a. Medical Instruments

It is estimated that the theft of equipment and supplies costs hospitals $4,000 per bed each year and with over 975,000 staffed beds in the United States, this represents a potential loss of $3.9 billion annually [28]. If each of these instruments is embedded with an RFID tag for real-time tracking, not only can they be prevented from getting stolen. They can also be located easily at times of emergencies.

b. Surgical Tools

After an operation, the surgeons always fear about a surgical instrument being left sewn-up inside the patient's body. Figure 15 illustrates the benefits of having a small RFID tag on each of the surgical tools and equipment and how it will enable the doctor to track each and every piece of equipment and eliminate this fear from the doctor's mind. The doctor can therefore concentrate more on the operation itself.

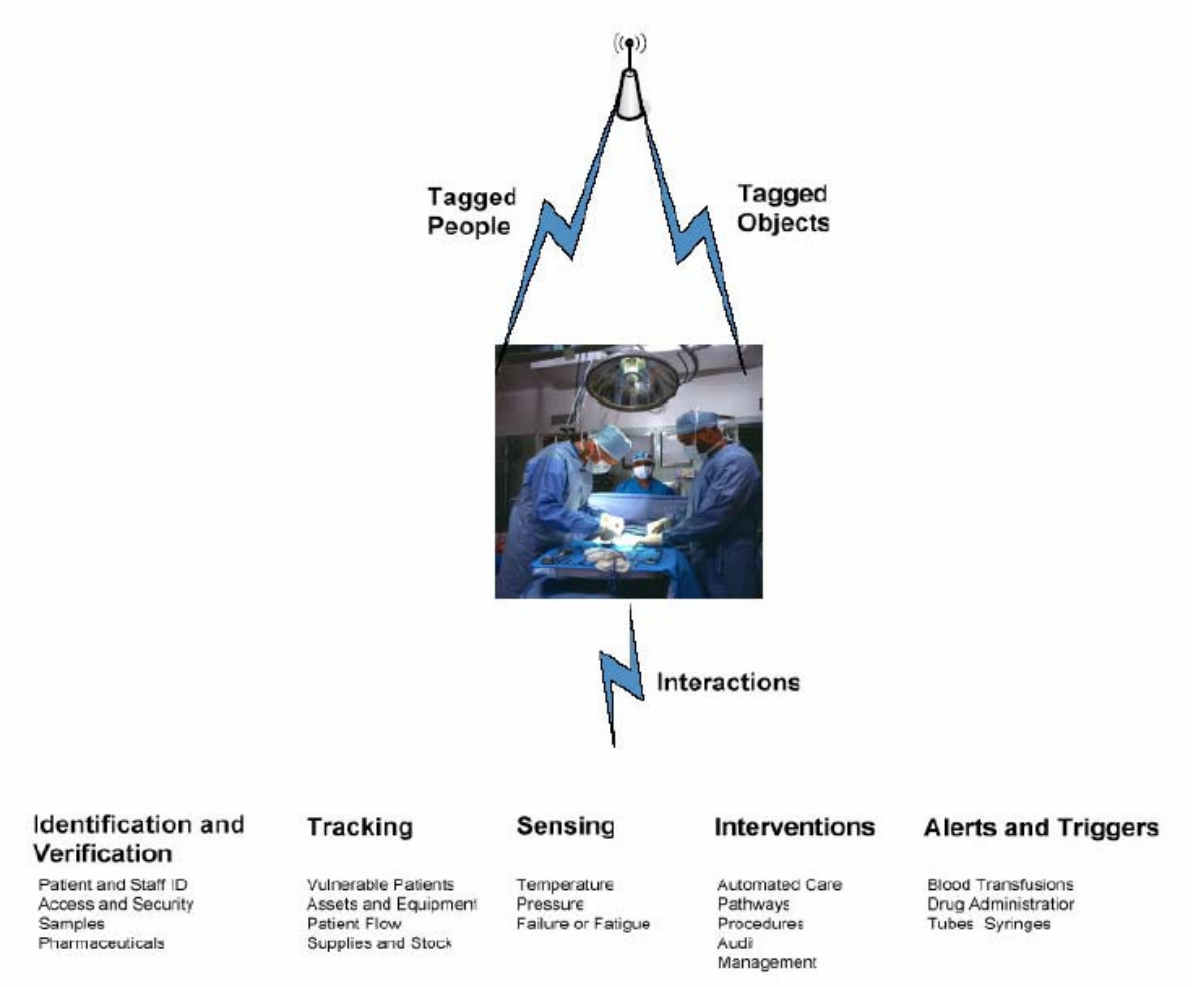


Figure 15. Tracking Surgical Tools Using RFID.
From: [29]

c. Other Miscellaneous Items

Items that are used by patients on a rotation basis need to be tracked for tracking a contamination. For example, a bed sheet in a hospital is randomly allocated to a bed after its routine visit to the laundry. If the bed sheets have an embedded RFID tag, all the dangerous infections can be tracked and the infected sheets can be either sterilized or simply disposed off.

3. Medicines and Drugs

a. Combating the Growth of Counterfeit Drugs

The Food and Drug Administration (FDA) estimates that up to forty percent of medicines shipped from countries such as Argentina, Colombia, and Mexico may be counterfeit [30]. Counterfeit drugs are a huge problem to our society and should be eliminated. RFID is commonly believed to be the best medicine against counterfeit drugs. Item-level RFID tagging can help eliminate this problem. The RFID tags located on the packages can be tailored to capture specific information required by the laws of the different states or countries. The requirement of all the information contained in the RFID tags should reduce counterfeits significantly.

b. Prescription Adherence

About forty percent of patients do not take their medication as prescribed according to Information Mediary Corporation (IMC) [31]. By using RFID tags on the packages of the medicines, the time of opening up the packages can be tracked. This information can be linked to the patient to prevent any bad effects arising out of not taking the medicines on time.

The effects of the drug can also be tested efficiently and more accurately using RFID tags. Each test person's data is captured into a computer including the times that they took the medication and the amount of medication he/she received [Figure 16].

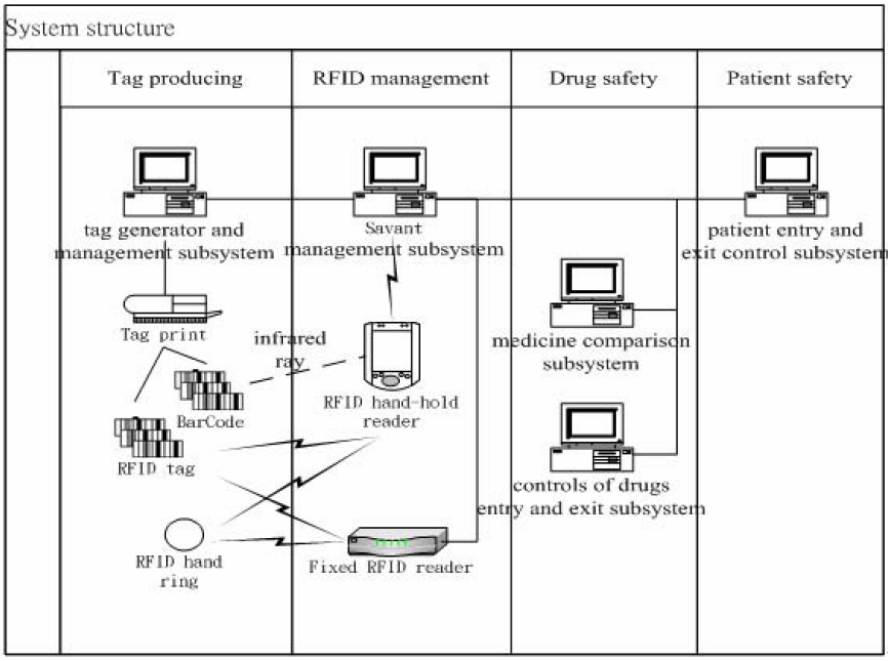


Figure 16. System Structure of Medicine Safety.
From: [32]

4. Miscellaneous Items

a. Specimen Bags, Slides, and Tubes

There can be medical errors related to inaccurate matching of a sample to the correct patient. The importance of positive patient identification (PPI) in reducing medical errors becomes clear when considering that between 44,000 and 98,000 patients die in the United States each year from medically-related errors [26]. The leading cause of death due to medical errors is caused by patient misidentification, and specimen or medicine misidentification. This cannot only be reduced, but eliminated altogether by the use of RFID. RFID tags can be placed on test tubes, slides and bags meant for holding test specimens and can be uniquely and accurately linked to a patient's records.

b. Blood Bank

Human blood has always been and always will be a precious commodity whenever a disaster occurs, or whenever a medical condition exists that requires a blood donation to prolong a person's life. Having that blood in the right place at the right time is critical to sustain the survival of the person in need.

Current military blood program uses a system called Joint Medical Asset Repository (JMAR) to oversee the blood donation and distribution. After the attacks of September 11, 2001, the Department of Health and Human Services (DHHS) had to rely on paper, pencil, phone, and fax to activate emergency plans to transfer medical volunteers and supplies to New York City [33]. According to Colonel G. Michael Fitzpatrick, Director of the Armed Services Blood Program Office, there is no nationwide computerized network for over half of the nation's blood donations. Within the DoD, the Defense Blood Standard System (DBSS) uses a client/server architecture to help the facilities track their blood supplies. These systems are strictly used in-house and do not have the interconnections with other DoD facilities to facilitate tracking and distribution of blood units and components.

During blood donation, DoD process involves requiring a blood donor to fill out an initial questionnaire that contains a barcode at the bottom of the card. Upon completion of the questionnaire, it is reviewed to ensure the prospective donor meets the donor qualification criteria. Once the donor is considered qualified to donate blood, the barcode is then removed from the form and attached to the blood bag that will be used for collection. From the collection point, the unit of blood is sent to the laboratory for processing and blood components such as plasma, platelets, and packed red blood cells are harvested. A barcode is attached to each of these components that will be used to trace back to its initial donor. Upon completion of the production and quality assurance procedures, a Food and Drug Administration (FDA) label that contains yet another barcode is attached to each of the blood components until the unit is dispensed for patient use.

Using RFID, the manufacturer of each bag produces the empty bags with an RFID tag embedded within it. Once the blood donation site receives the bags, all they have to do is write to the tag the type of blood, where the blood was donated and collected from, and the name of the donor. With this information written to the tag, donated blood can be tracked through RFID readers as it is distributed and administered to the patients. RFID implementation can also use the temperature-sensing tags that can be used to track the temperature history recorded on the chip. This alerts the medical personnel if the blood unit reached an unsafe temperature through its short life span.

Using temperature-sensing tags dramatically reduces the probability of using spoiled blood that may have been exposed to temperatures that affect the viability of the blood components for sustaining life functions.

c. Medical Waste

The medical wastes coming out of a hospital are extremely hazardous. These wastes can be easily tracked by the waste management agency with the help of RFID. All hospitals have to do is put an RFID tag on all outgoing waste bags. The waste management agency can then easily detect the presence of medical waste in the surroundings and appropriately treat it before it becomes dangerous to the population.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SYSTEM ARCHITECTURE REVIEW

A. RFIDLOCATOR

1. Introduction

The basis of the idea behind the RFIDLocator satisfies a concrete need for many companies: "Given a set of objects constantly moving in a predefined area, where can we find them at a given time *t.*" This application is not primarily intended for asset tracking within the supply chain as most RFID systems do. Rather, it is aims to locate tagged objects or individuals moving within a defined area of coverage.

To clarify the usefulness of this application, the following hypothetical situation can be considered:

> Good Health Nursing Home employs more than 20 health professionals to provide the healthcare needs of 250 patients. Every medical procedure and progress notes pertaining to each patient are documented on paper records manually maintained and updated throughout the patient's stay at the facility. As patients are transported in and out of the facility for medical procedures and testing, their records are also transported with them to provide current medical history to the referred healthcare provider and for them to record progress and treatment documentation. Since paper records can potentially be misplaced or lost, the nursing staff could spend significant amount of their time searching for the missing patient record which may delay the patient's transport incurring higher cost for transportation and even resulting in a cancellation of the procedure and the patient not receiving the prescribed procedure on time.
>
> This problem could be solved by purchasing a few RFID readers, paste RFID labels onto each patient record and set up a software application that could track the patient records as patients are moved around.
>
> The nursing staff would only need to query the application on the location of any patient record and eliminate the waste involved in the physically searching the whole facility.

This case reflects a real need for an automated way of tracking documents within the confines of any facility.

2. Object Model

To introduce the terminology used within the RFIDLocator application, Figure 17 lists and describes the object model used in the application.

a. Location

The Location object models a place (i.e., a building, a room, a shelf, a desk) within the area controlled by the RFIDLocator. It is identified by a unique

Business Location Number. The Location is the central object of RFIDLocator as it aims to locate physical objects. This is to answer the question: Given a physical object to look for, in which registered Location did it go through? As a consequence, the LocatorObservations (i.e., observations that are valid in the context of RFIDLocator) are always linked to a Location.

b. TraceableObject

Such an object is a physical element that can be tracked by RFIDLocator. It could be about anything that is physically big enough to hold an RFID tag. The TraceableObject is the integration point between the legacy business system and the RFIDLocator application. The TraceableObject contains two fields that uniquely identify the object:

(i) One on the business system side: the businessNumber (i.e., Case-Gu-2411).

(ii) The other on the RFIDLocator side: the epcString (i.e., urn:epc:id:gid-96:1.1.150).

The use of both these unique identifiers enables an object to be searched by businessNumber even if the latter is actually identified using its epcString for the RFIDLocator application and its attached readers. A TraceableObject is always attached to the User who registered it. Depending on the policies of the organization running the RFIDLocator software, displaying it when querying for the location of an object could be of great help. In some cases, the User is likely to have a better knowledge of where the TraceableObject might be located.

c. User

A User is basically someone allowed to access and query RFIDLocator. This version of the application does not distinguish the users accordingly to their respective rights (administration, querying, etc.). Yet the reader should note that this fact could be of great relevance in a commercial application.

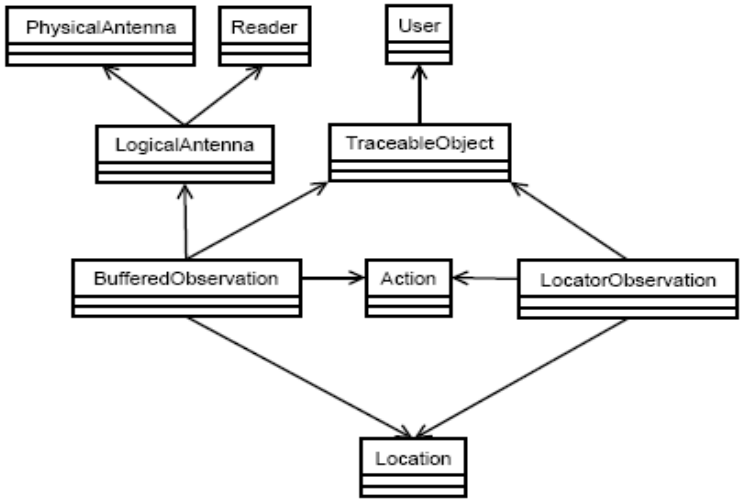


Figure 17. The Object Model of the RFIDLocator.
From: [34]

d. LocatorObservation

It is the persistent result of an RFID event. Its semantics is basically that a TraceableObject was observed at a given time going IN or OUT of a particular Location. When tracing TraceableObjects, the queries will be made on these objects.

e. BufferedObservation

An observation is basically a potential LocatorObservation. It is used by the solving algorithms when elements are missing to actually "persist" the Observation. Unlike a LocatorObservation, each of these objects is connected to a LogicalAntenna. This can be explained by the fact that the algorithms solving the Observations are commanded by the LogicalAntennae.

f. Action

An Action is the fundamental element for the algorithm that traces physical objects. This version of the RFIDLocator supports two actions: IN and OUT. An IN on a Location means that the object entered the Location, whereas an OUT means that the object exited the Location. The INs and OUTs are distinguished at the PhysicalAntenna level. A PhysicalAntenna is always attached to either an IN or an OUT Action.

g. LogicalAntenna

A LogicalAntenna is an aggregate of PhysicalAntennae. It is used to determine what Action (i.e. IN/OUT) was effectively recorded by the n PhysicalAntennae. The LogicalAntenna16 is thus the central component in the solving of an Observation. It is always associated with a Location.

h. PhysicalAntenna

A PhysicalAntenna represents the hardware able to capture RFID events by producing an electro magnetic field. An antenna is not a standalone unit; it is always connected to a Reader. A PhysicalAntenna must be identified by an EPC (or another type of unique identifier). Additionally, a PhysicalAntenna is always connected to a LogicalAntenna.

i. Reader

An RFID reader is a physical hardware device controlling a set of PhysicalAntennas which detect tagged objects within their fields.

3. Use

The requirements of the RFIDLocator application are best addressed using distributed software architecture. The need to be able to use it from anywhere and not just on the computer which processes the observations is a critical reality. Its Graphical User Interface (GUI) is a web-based thin-client. The application is accessible by typing the application's Uniform Resource Locator (URL) in the address bar of the web browser. The welcome page of the application is shown on Figure 18.

Figure 18. Thin-Client GUI of the RFIDLocator.

From: [35]

The main menu is placed on the left and a quick access to the functionalities is provided in the bottom of the page. The content of the page is displayed in the "body" of the page with the upper right corner containing the navigation tools to guide the users of the application. The main functionalities accessible using the menu are briefly described as follows:

a. Create a New User

This link permits to create a new user. All the fields are required. Once the form is filled and submitted, the new user can login via the home page.

b. Configure the Environment

This page is required to set the initial environment of RFIDLocator. An XML description of which reader is located where has to be provided in the text field. The syntax of the XML that must be used is described in Figure 19.

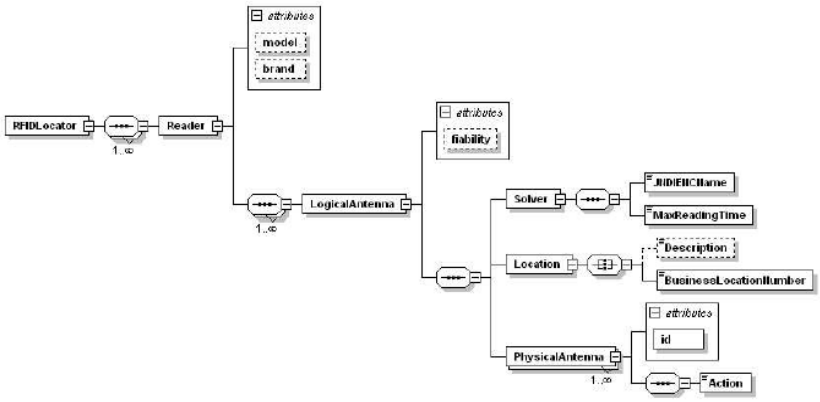


Figure 19. Diagram of the XML Syntax.

From: [36]

Figure 20 provides a screenshot of the readers' configuration page.

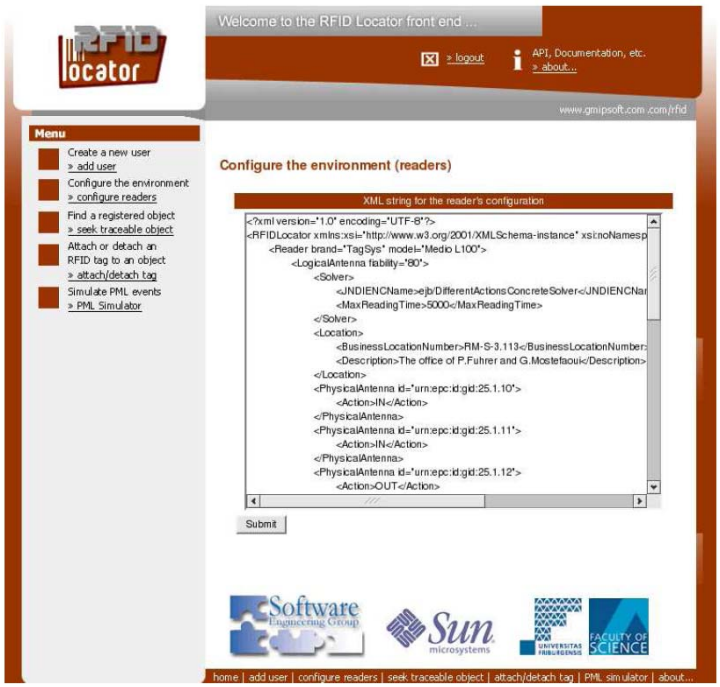


Figure 20. Reader's Configuration Page.

From: [35]

c. Attach/Detach a Tag

To inform the RFIDLocator that it should trace an object, one needs to attach an RFID tag to the object both physically and virtually. First, the user enters the BusinessNumber which is a unique string that the company uses to identify the object (i.e., case JP guinard 05 or portable computer 0205). The user enters the unique number of the RFID tag. It corresponds to the unique number recorded on the tag that is physically pasted onto the object. Finally, the user can choose between Attach and Detach. The former binds the tag ID to the BusinessNumber, creating a TraceableObject. The Detach function deletes a TraceableObject from the system. Only the BusinessNumber is mandatory when Detach is selected. Once a tag is attached to an object, it becomes a Traceable Object and can be traced by RFIDLocator.

d. Find a Registered Object

This permits the user to seek a Traceable Object by providing its Business-Number. The system will return all the observations the RFID readers made from this particular object. Figure 21 presents the results of a typical seeking query.

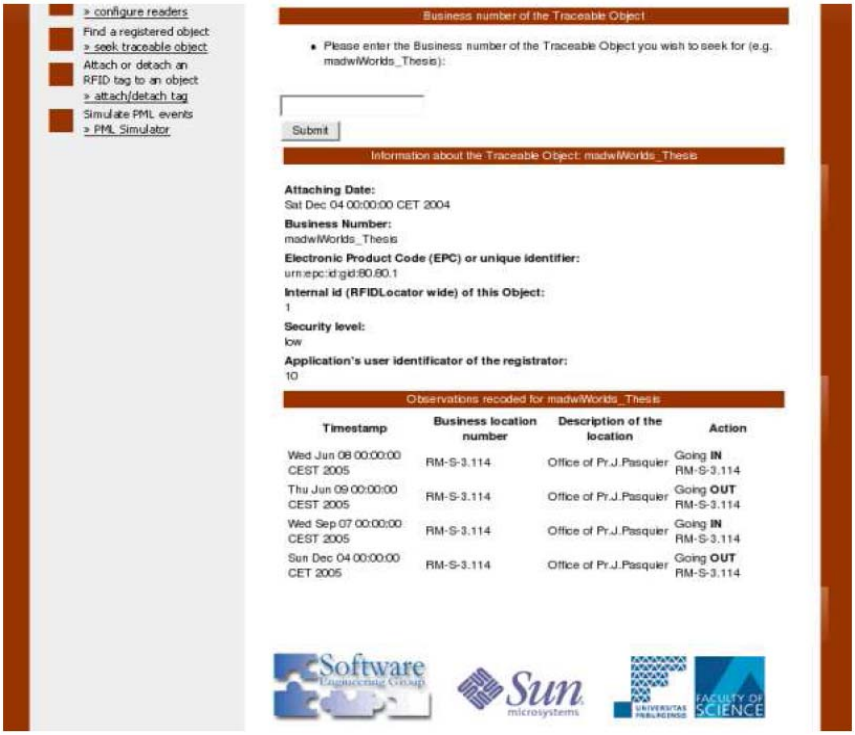


Figure 21. Seeking a Traceable Query.
From: [35]

e. Simulate PML Events

This page offers to simulate the events reported by an RFID reader. It permits to test the application without having an actual physical reader. The user is prompted for a PML string that describes an observation.

4. Technological Choices

Various software platforms were considered for the development of RFIDLocator. The field of choices was considerably large but the attention was focused on the following design that met the parameters for implementation.

a. Event Manager

The first software component required for an enterprise application working with RFID and EPCs is an implementation of the Event Manager. This software is available on the market but not all of them meet the Savants' standards articulated by EPCglobal. Several software vendors provide flexible and standard compliant RFID middleware such as IBM and its WebSphere RFID Premises Server, Oracle and its RFID and Sensor-Based Services, the RFID application proposed by SAP as an extension of its well known ERP, or the Sun Java System RFID Software. RFIDLocator was designed using Sun's implementation of the Event Manager which is one of the first of Savant's implementation on the market.

b. Enterprise Java Beans

Many technologies propose to solve the problem of distributed computing. Among these, two technologies are leading the field in providing the enterprise applications with robust and reliable software. The first is the .NET Framework by Microsoft Corporation and the other is known as J2EE. In the interest of using a technology that supports open standards, the J2EE and its "EJBs" (Enterprise JavaBeans) was adopted due to the fact that it is managed by an application server that offers a complete and integrated solution for the persistence layer. It also makes the integration of JMS messages easier and reduces development effort by providing services for dealing with critical issues such as scalability, concurrency and security.

c. Application Server and Database

The Application Server is a software on which a J2EE application can be deployed. Because of the EJB specification, the choice of an Application Server should not be an irreversible decision. Any Application Server that implements the EJB specification would theoretically be able to run the RFIDLocator without any changes or after some minor changes. The RFIDLocator is best designed for the Sun Java System Application Server coupled with the bundled PointBase Relational Database Management System (RDBMS).

Figure 22 shows the respective role of the Event Manager and the Application Server in the RFID application. Besides these software choices, adapted RFID hardware (readers, connectors, servers, RFID tags) must also be selected.

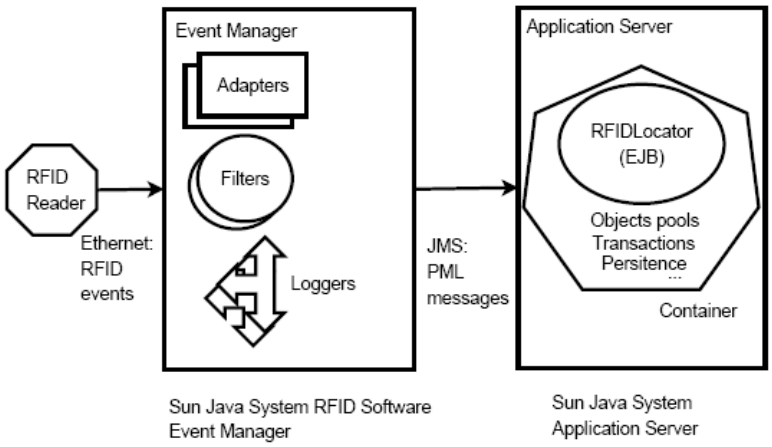


Figure 22. Event Manager and the Application Server. From: [35]

Figure 23 depicts the physical deployment of the different parts of this distributed application.

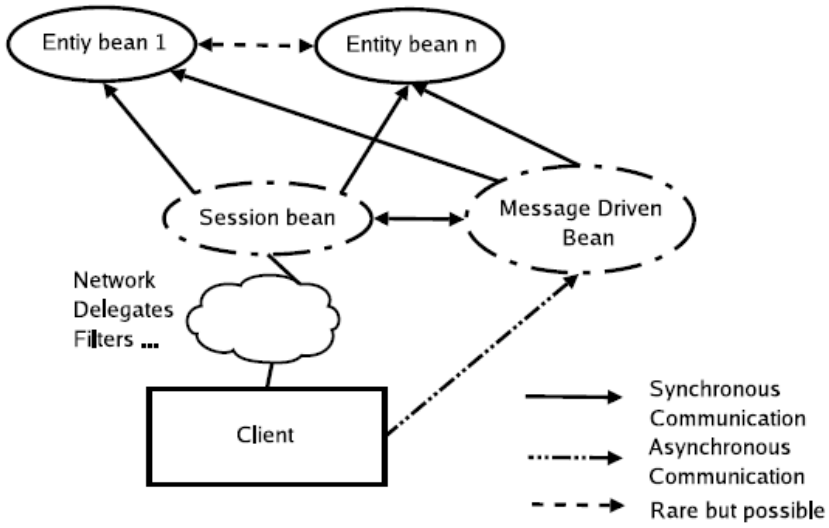


Figure 23. Elements of the EJB Framework.
From: [37]

5. Software Architecture

RFIDLocator contains more than a hundred classes. The core of the application is built around the relatively small set of objects that are implemented as Entity Beans (Entities) and represent actual data in a storage medium. In this case, the Entities represent tuples in a relational database. On the other hand, Session Beans (Sessions) contain the specific business logic of the application.

RFIDLocator proposes several Session Beans offering business services. The place of the Session Beans in the overall EJB framework is shown on Figure 23. Session Beans are accessed by the client through a number of interfaces and proxies to solve a business task. The Sessions are interacting with Entities to for direct access while gaining access to other Entities at the same time.

The following terms are used to describe the interactions between the Sessions and the Message-Driven Entities:

a. Users

The UserManagerSessionBean offers methods related to the management of RFIDLocators. As an example, the method registerUser() can be used to add a new user to the system.

b. Location Manager

This Session Bean is intended to offer methods regarding the places within the predefined area covered by the application. The method addLocation() provides a way of creating a new Location. The newly created Location is going to be part of the places RFIDLocator can monitor (provided a PhysicalAntenna is placed in this Location). It is primarily intended to be used by other Session Beans (such as the SensorManager SessionBean).

c. Traceable Object Manager

The TraceableObjectManager offers methods for managing the objects that can be traced by RFIDLocator such as the TraceableObjects. It also provides a central method called locationHistory() which is in charge of returning the Locations a TraceableObject went through. This service is the core business of the RFIDLocator application as it permits the approximation of the current place an object is in.

d. PML Simulator Publisher

To test the system without the need for many RFID readers, RFIDLocator is provided with a PMLSimulatorPublisher. This Session offers methods to simulate the sending of Java Message Service (JMS) PML events. To convey these messages, it provides the publishPML(String PMLCoreString) method.

e. Observation Manager

The ObservationManager is in charge of persisting Observations using the method addLocatorObservation(). An observation has to go through various steps before being identified as a LocatorObservation.

f. Reader Manager

This Session Bean provides a method for parsing an XML file containing the settings of the environment in which RFIDLocator has to be deployed. The method parseConfigString() takes an XML string as argument and builds an object graph containing the following elements: (i) Readers; (ii) LogicalAntennae; (iii)

PhysicalAntennae; (iv) Solvers; (v) Locations. The syntax of the stream to be parsed is defined by an XML schema. The transformation of the input string into a set of objects is achieved by using Sun's implementation of the Java Architecture for XML (Data) Binding (JAXB). This specification enables the conversion of an XML document into Java Objects in a very straightforward manner. In this particular context, the conversion is called unmarshalling to Content Objects. Figure 24 provides a schemed view of this process. Eventually, after creating the Content Objects the ReaderManager "persists" them into the corresponding Entity Beans.

g. Sensor Listener Message Driven Bean

The SensorListener is the integration point between the Event Manager and the final application (Figure 25). The events reported by the Event Manager go through several steps ending to a JMS Queue called the RFIDLocatorQueue. The SensorListener is a Message Driven Bean (MDB) listening to this queue which is being notified by the EJB container each time a message is posted on the RFIDLocatorQueue.

A message arrives at the MDB in the form of a PML string. The PML is then unmarshalled using the JAXB API. Upon conversion, the Message Driven Bean does the first filtering by checking whether the PhysicalAntenna that made the Observation is registered within the RFIDLocator. If this is the case, the SensorListener contacts the corresponding LogicalAntenna and asks it to solve the observation by deciding what to do with the incoming observation. The EJB container automates all the receiving and listening overhead which enables the system to concentrate on the business logic of the asynchronous component.

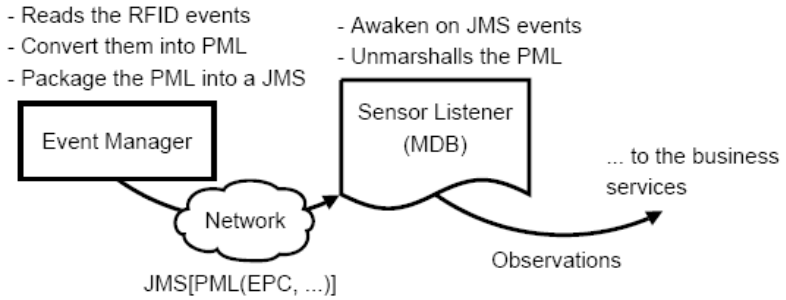


Figure 24. Marshalling/Unmarshalling Process of the Reader Manager. From: [37]

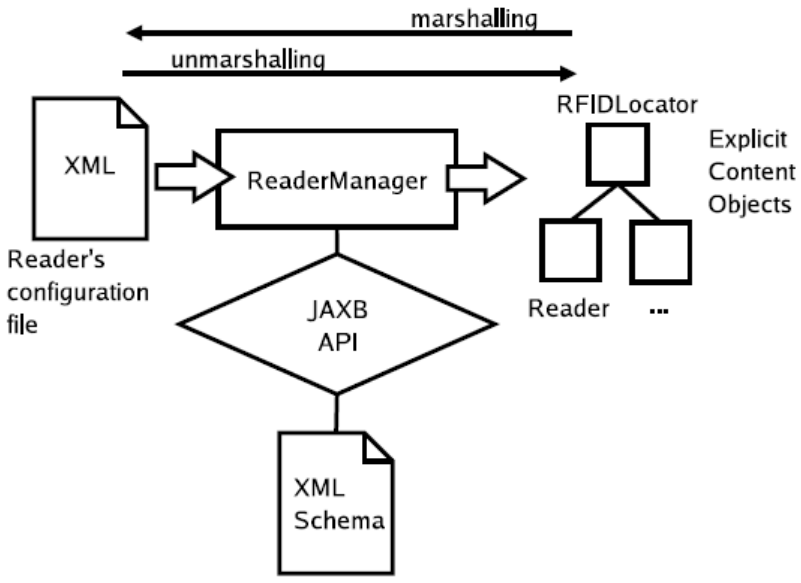


Figure 25. Asynchronous Communication Between EM and the Application. From: [38]

h. Solvers

The Solvers implement the algorithms used by RFIDLocator to trace the position of the TraceableObjects. When a message arrives at the JMS Queue of the application, the Sensor Listener Message Driven Bean contacts the corresponding LogicalAntenna (Figure 26) and asks it to solve the incoming Observations by invoking its SolveObservation() method. To do so, the LogicalAntenna passes the Observations to its Solver. According to the algorithm it implements, a Solver has three possibilities when handling an Observation:

- Persist the Observation as a LocatorObservation, which can be interpreted as a direct validation of the incoming Observation.
- Buffer the Observation as a BufferedObservation in order to wait for some more information before actually taking a decision.
- Discard the Observation, which can be interpreted as declaring it to be invalid.

Solvers are available in many variations. To satisfy this criterion, the Solvers are based on the modular architecture depicted on Figure 27. The Solvers implement the ObservationSolver interface. The Solvers also define a single method called Solve (). This method is called by the LogicalAntenna using its concrete Solver when the validation of an Observation is required. To add a new Solver, one just needs to implement it and attach it to the LogicalAntennae. Two Solvers were developed for this version of RFIDLocator. Both of them are implemented as Session Beans because of the high performances of these components as well as its convenient integration with the final application.

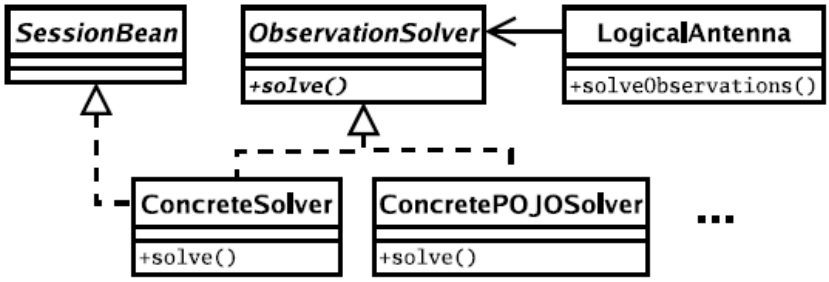


Figure 26. Logical Antenna and Observation Solvers.
From: [38]

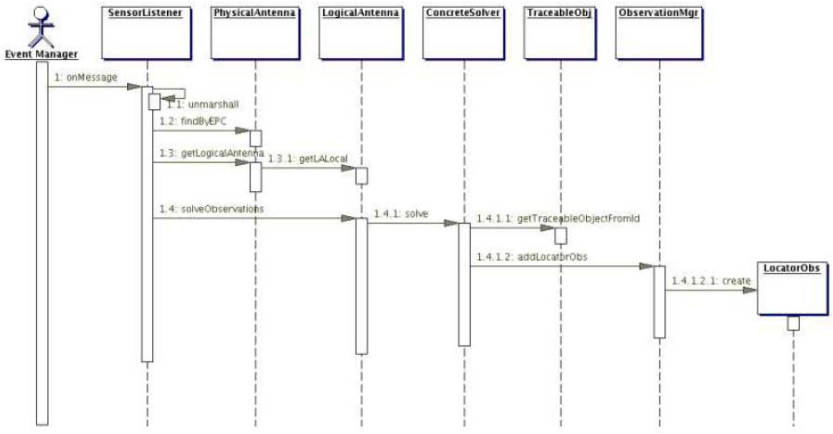


Figure 27. Sequence Diagram of an Observation Solved Using a Simple Concrete Solver.
From: [35]

A fully configured RFIDLocator system is represented in Figure 28.

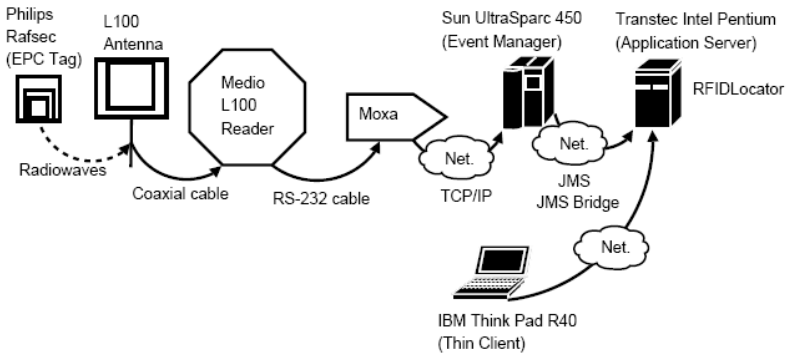


Figure 28. RFIDLocator Device Configuration.
From: [35]

6. Summary

RFIDLocator is a fully functional open-source J2EE application that allows the ability to locate and trace electronically tagged objects and individuals within a predefined area. RFID is the underlying technology used to achieve this goal. The adoption of the standards of the RFID field, as well as the use of established Java enterprise framework are prerequisites to build a scalable, robust and reliable application. The clean, flexible and well-documented software architecture of the RFIDLocator allows interested people to extend it to fit their particular requirements.

B. SENSOR NETWORKS

1. System Requirements and Network Architecture

A main issue for machine-to-machine communication is that the flow of information differs substantially from that in present-day computer networks. Instead of a large flow from central servers to clients at the edge of the network, the main data flow for RFID and sensor network systems is from many devices at the edge of the network towards a few central servers. This is especially true for condition-based maintenance sensor networks and RFID networks at manufacturers and distribution centers. In both

systems, sensors or RFID readers detect certain events and forward the corresponding information to some business application on a central server. The business application then responds to these inputs and arranges corresponding actions such as replacing a fragile component before it fails or requesting the delivery of additional products before they are sold out. For both kinds of networks, this creates an imploding data stream from the edge to the center. To handle this kind of data streams for a large number of sensors or RFID readers, data or event filtering as well as data aggregation and abstraction are necessary at all suitable points from the edge towards the center of the network. Therefore, certain parts of the business application are transferred from central servers to those at the edge of the network. To enable fast implementation of new applications, a flexible and automatic deployment of software on the edge servers is necessary. RFID systems at points of sale or access-control and sensor networks for real-time process control require actuators for automatic responses in addition to RFID readers and sensors. Depending on the acceptable response time, decisions on corresponding RFID reader or sensor data are made at central servers or directly at the closest edge server or sensor controller. If short response times are required, significant parts of the application must be running on the edge server or sensor/RFID controller, thereby shifting intelligence and responsibility from the network center to the network edge.

Other system requirements are remote device configuration, remote device software updates, system diagnostics including sensor diagnostics, network reliability and security, and application access to data on a by-topic base instead of a per-device base. The requirements for remote configuration and software updates stem from the possibility that very large number of edge devices and the fact that many of these devices will be installed far away from any information technology knowledgeable staff. Under these conditions, the total cost of ownership of RFID and sensor networks becomes unacceptable without remote system management. The requirement for real-time system diagnostics and overview is a simple consequence of the fact that these networks provide mission-critical inputs to business applications. Also, business applications usually need to know data according to specific topics, such as manufacturer information according to RFID electronic product code (EPC), temperature, pressure, or other parameters, and not according to which device measured the data. An intelligent network infrastructure

should provide the corresponding data automatically in the way the applications need them. Depending on the applications, customers will require various degrees of network reliability and security. For most RFID and sensor networks, the important issue will be network reliability and data integrity in such a way that there should be no network breakdowns due to failing components or external denial-of-service attacks, and information received from the network should be reliable. Protection against failing components will require redundant designs of critical network elements, whereas data integrity and protection against denial-of-service attacks will require device and message authentication.

A suitable architecture for RFID and sensor network backbones is shown in Figure 29. Here, SU means a sensor unit or RFID reader with a wired or wireless connection to a gateway (GW), and AU means an actuator unit for automatic response actions. The gateway is a sensor or RFID controller which can connect to the normal enterprise network. It will usually be based on a 32-bit microprocessor but depending on the application, the capabilities of the gateway may still be limited by power-consumption constraints in situations that there may be no local storage capability at the gateway. The first possible point for data filtering, aggregation and abstraction is at the gateway, except for the case where a mesh network of sensor units is connected to the gateway and some kind of data aggregation and filtering is already done within the mesh network.

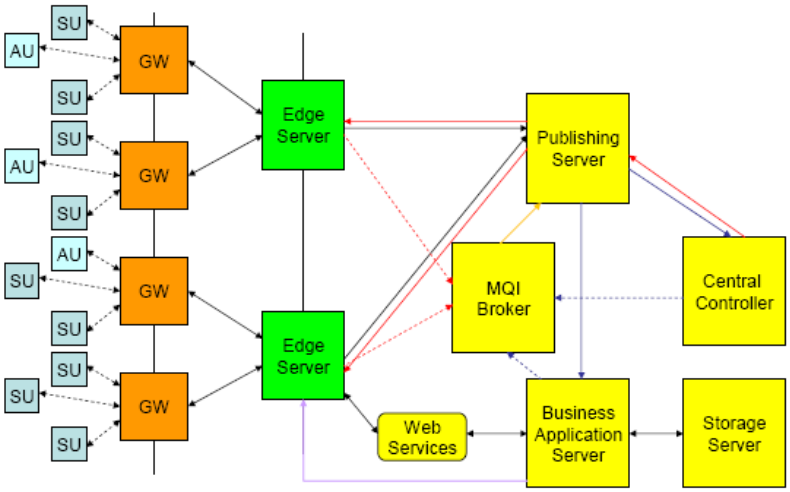


Figure 29. Sensor Network Architecture.
From: [39]

The next level of data aggregation and abstraction is performed at the edge servers. To enable flexible deployment of application codes from central servers to edge servers or even gateways, the software architecture of these devices uses IBM's Service Management Framework (SMF) which is based on the standards of the Open Services Gateway initiative (OSGi).

Figure 30 shows corresponding software architecture with a Java virtual machine as basis. SMF enables receiving of software code bundles from a central server and updating application code and configuration information. This software architecture is suitable for edge servers, high-performance gateways and RFID controllers. Some gateways for remote sensor network applications with serious power consumption and related memory constraints may not be able to support the complete software architecture of Figure 30. Nevertheless, all gateways should still be able to support a slimmed-down version based on the J9 Java virtual machine for embedded systems plus the Message Queue Telemetry Transport (MQTT) protocol for reliable message transport between gateways, edge servers, and central servers. Publish and subscribe functionality works by pushing data with MQTT to specific central servers for publishing data in specific formats to specific applications and servers based on subscription lists. These subscription lists are created by a central MQ integration (MQI) broker to which all

applications send subscription requests defining what data they want to receive and in which format. The gateways on the other hand can subscribe to configuration updates concerning all sensor units or RFID readers connected to them. This enables efficient remote device configuration.

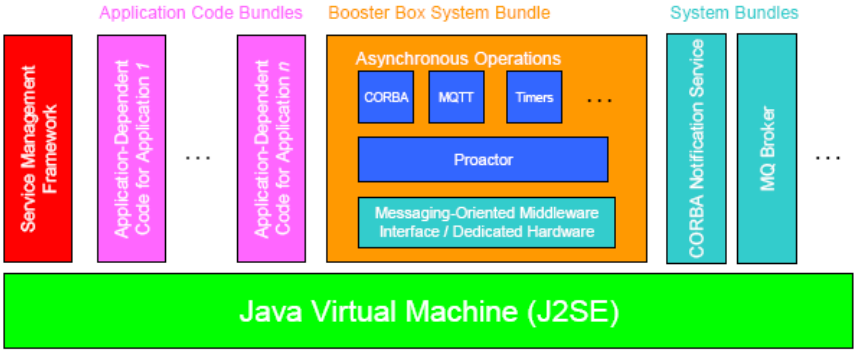


Figure 30. Software Architecture for Code Updates.
From: [40]

Access to web services for supply-chain optimization beyond single companies or EPC information access is possible from edge and central servers. Device and message authentication between queue managers is an integral part of IBM's MQ middleware, and creates the basis for end-to-end system security in RFID and sensor networks based on the architecture shown in Figure 29.

2. Smart Sensor Devices and their Integration into the Network

There are three main classes of RFID reader and sensor devices. The first class is that of wired devices with no serious power constraints. These devices will usually include physical sensors or RFID readers, plus a 32-bit microprocessor for local data processing and a network connection. They are a combination of sensor unit and gateway or RFID reader and RFID controller. Main applications are fixed installed RFID readers or wired sensor units for real-time process control in industrial automation.

The second class is that of PDA-like battery-driven mobile devices as RFID readers or smart sensor units. They are nearly identical to the wired devices but use wireless connections to the backbone network. Their main applications are RFID-based

inventory control, personal smart sensor systems for medical control and remote condition-based maintenance systems that are switched on just once or twice per day. Battery lifetimes for the RFID and personal smart sensor systems will be comparable to those of mobile phones. Acceptable battery lifetimes of about 10,000 hours for the condition-based maintenance systems are achieved through extremely low duty cycles for these systems.

The third class is that of battery-driven, very-low-power, low-performance smart sensor units. These devices include physical sensors plus a low-power (usually 8-bit) microcontroller, very little memory, and a low-power, small-range wireless radio connection. Battery lifetimes of 10,000 to 15,000 hours are achieved with duty cycles of about 0.01%. These systems are in sleep mode about 99.9% of their time. These units need a gateway to connect to a usual computer network. For now, there seems to be no counterpart in RFID systems for this class of devices [39].

Devices of the first and second class are easily integrated into standard computer networks because they can use standard embedded software solutions such as the one shown in Figure 30.

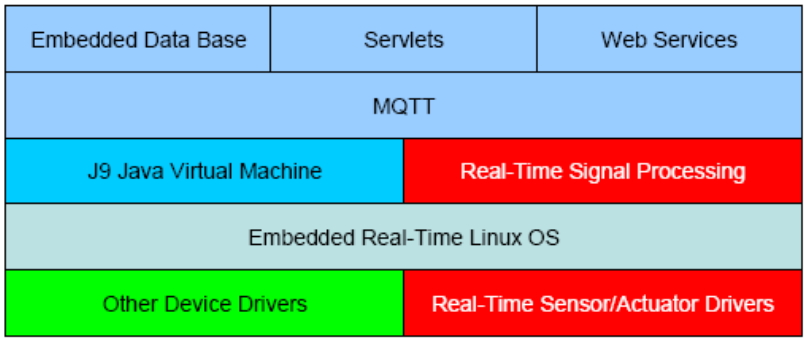


Figure 31. Software Architecture of Real-Time Sensor Controller. From: [42]

The software architecture of Figure 31 supports MQ-based connection to the backbone network as well as access to the Internet through web services. It is therefore completely compatible with the architecture given in Figure 29. The real-time signal-

processing application runs directly on embedded Linux instead of on the Java virtual machine to enable very fast feedback.

Devices of the third class pose more difficulties for integration into a complete system solution with end-to-end security and service guaranties because they are based on highly application-specific software usually running on 8-bit microcontrollers. Examples of operating systems are TinyOS from the University of California at Berkeley and the IEEE 802.15.4 [11] protocol stack extended by the ZigBee industry alliance recommendations. The complete protocol stack for TinyOS is about 3.5 KB and that of the IEEE 802.15.4/ZigBee standard about 4KB for simple sensor network nodes. Nevertheless, at least end-to-end system security should be feasible as the IEEE 802.15.4 standard supports symmetric key encryption and authentication.

C. AUTHENTICATION PROCESSING FRAMEWORK

1. Introduction

Many proposals have been presented to deter the privacy and security problems involved in RFID technology; however, those proposals have one disadvantage or the other and these had made them insufficient to completely address the problems. A simple approach for dealing with the privacy concerns might be to prevent readers from receiving data coming from tags. The following will briefly describe some of the approaches and their adverse effects:

a. Kill Command Idea

The standard mode of operation proposed by the AutoID Center is for tags to be killed upon purchase of the tagged product. With their proposed tag design, a tag can be killed by sending it a special “kill” command but there are many environments in which simple measures like “kill command” are undesirable for privacy enforcement. For example, consumers may wish RFID tags to remain operative while in their possession.

b. Faraday Cage Approach

An RFID tag may be shielded from scrutiny using what is known as a Faraday Cage. It is a container made of metal mesh or foil which is impenetrable by

radio signals of certain frequencies. There have been reports that some thieves have been using foil-lined bags in retail shops to prevent shoplifting-detection mechanisms.

c. The Active Jamming Approach

An active jamming approach is a physical means of shielding tags from view. In this approach, the user could use a radio frequency device which actively sends radio signals so as to block the operation of any nearby RFID readers but this approach could be illegal. This could be applied in situations where the broadcast power is too high that it could disrupt all nearby RFID systems that could prove dangerous and cause problems in critical areas such as hospitals.

d. Blocker Tag Approach

The blocker tag is the tag that replies with simulated signals when queried by reader so that the reader cannot trust the received signals. Like active jamming, the blocker tag may affect the other legal tags in operation. All these approaches could have been great solutions to the privacy problem but the disadvantages make them unacceptable.

In consideration of the privacy concerns identified above, the Authentication Processing Framework (APF) could be considered the best option to provide the solution to the privacy problem and enhance the security in RFID system.

2. Concept

The main idea of the Authentication Processing Framework is that tags and readers will register with the APF database which will authenticate readers prior to when it will read the data in the tag. Implementing this kind of framework in the RFID system will alleviate the security and privacy concerns.

3. Overview

The APF was proposed to deter the data security problem in the RFID system. APF is a framework that makes it compulsory for readers to authenticate themselves with the APF database before they can read the information in the registered tags. Figure 32 denotes the four application segments that comprise the APF:

a. Tag Writer's Application

This is the part of the APF system that encrypts the information in the tag and produces the decryption key which will be submitted along with its identification number to the APF database.

b. The Reader's Application

The reader's application queries the tag and registers readers' identification number with the APF database. The reader's application also gets the decryption key to decrypt the encrypted information after it has been authenticated by the APF database.

c. Authentication's Application

This integrates both the reader application and the APF database maintenance application.

d. Maintenance's Application

This is the part of the system that maintains the APF database.

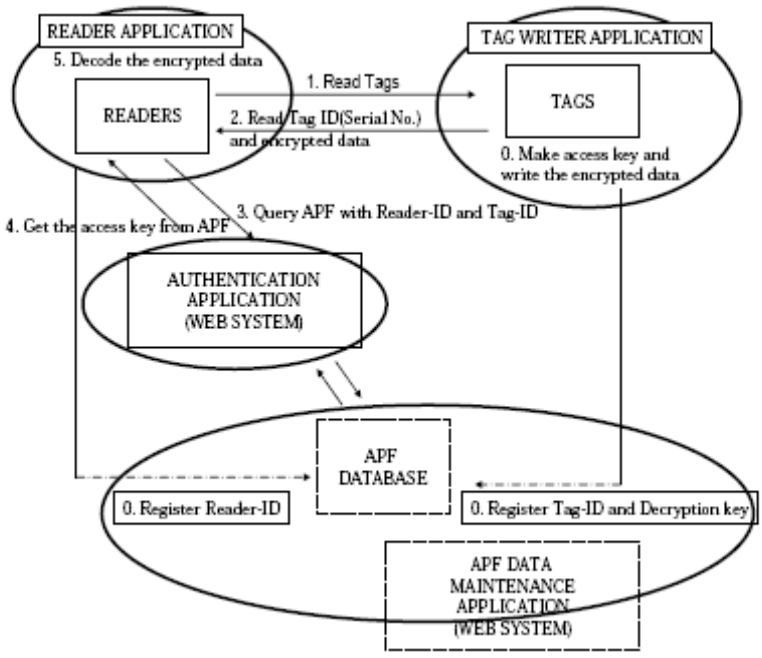


Figure 32. APF Functional Diagram.

From: [42]

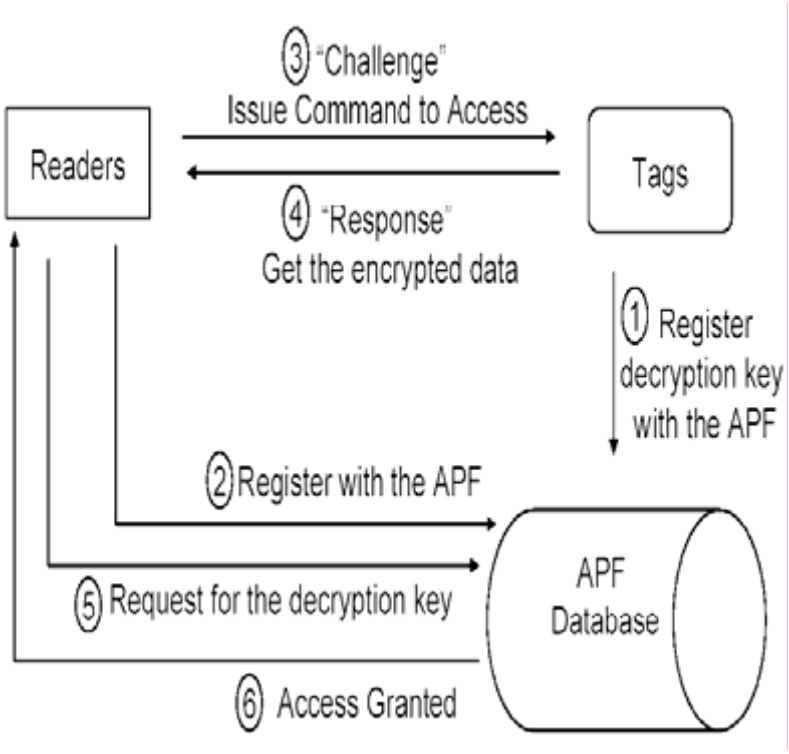


Figure 33. Flowchart of APF Framework.
From: [43]

4. Methodology

Figure 33 represents the step by step function of the APF system. Initially, the tags will register their identification numbers and the decryption keys with the APF database. The readers will register their identification numbers with the APF database. The readers will also send "Challenge" command to access tags. Using the APF system protocol, tags will send "Response" command which will be the tag identification number and the encrypted data to the readers. The response message from the tag will instruct the reader to get the decryption key from the APF database in order to decrypt and read the data in the tag. Since authentic readers would have registered with the APF database, only authentic readers would be given the decryption key to decrypt the encrypted data in the tags.

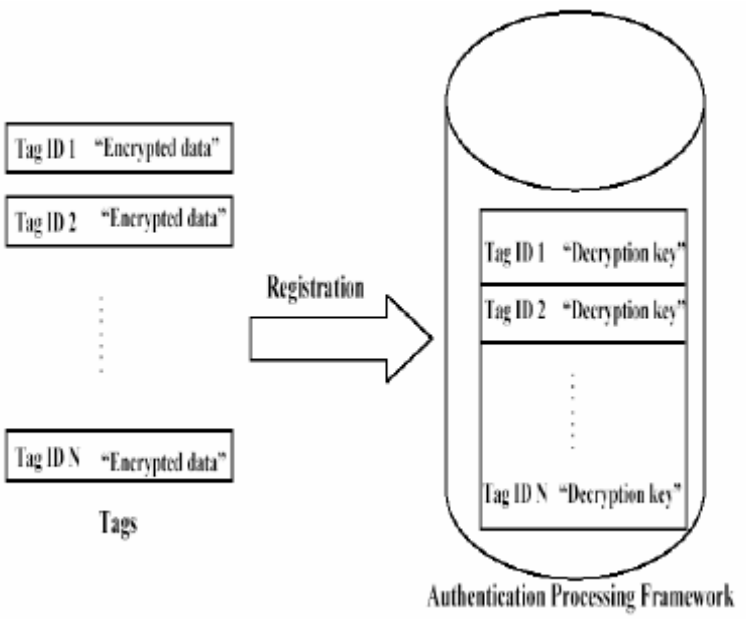


Figure 34. Transponder Registration of Unique ID Number and Key with the APF. From: [44]

To prevent illegal access to the information stored in the tags, there should be a procedural access control to the information stored in the tags. The unique ID and registration and the transmission of the decryption key is necessary for the protection of tag from unscrupulous readers [Figure 34]. Once the tag registers its unique identity and decryption key with the APF, it will be difficult for unregistered readers to have access to the tag data without possessing the decryption key. This means every registered reader will be authenticated prior to getting the decryption key to access stored data in the tag. Every reader will register its unique identification number with the APF and this will be confirmed by the APF before releasing the decryption key to the reader in order to read the encrypted data in the specific tag [Figure 35].

Since both readers and tags register their identification numbers with the APF, these serve as a mutual authentication and protect the information in the tags from malicious readers which is one of the concerns users have. This means that unauthorized access into the tag will be prevented using the APF.

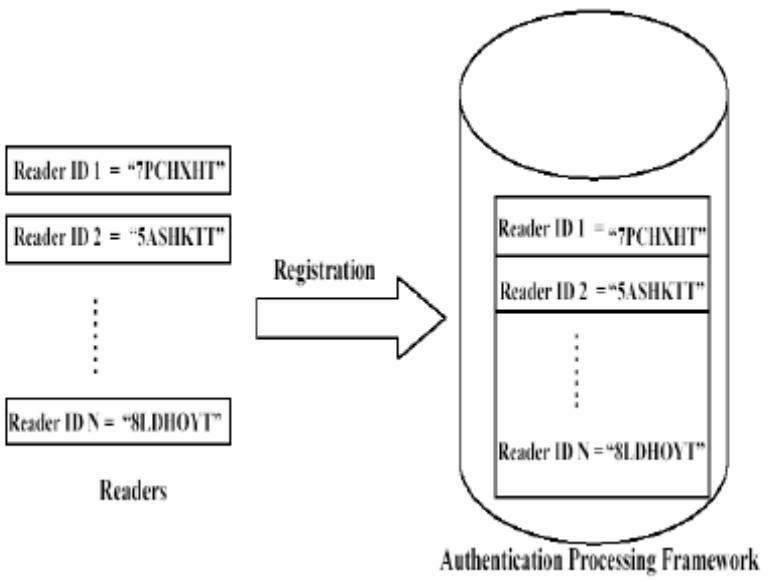


Figure 35. Reader Registration of Unique ID Number and Key with the APF. From: [45]

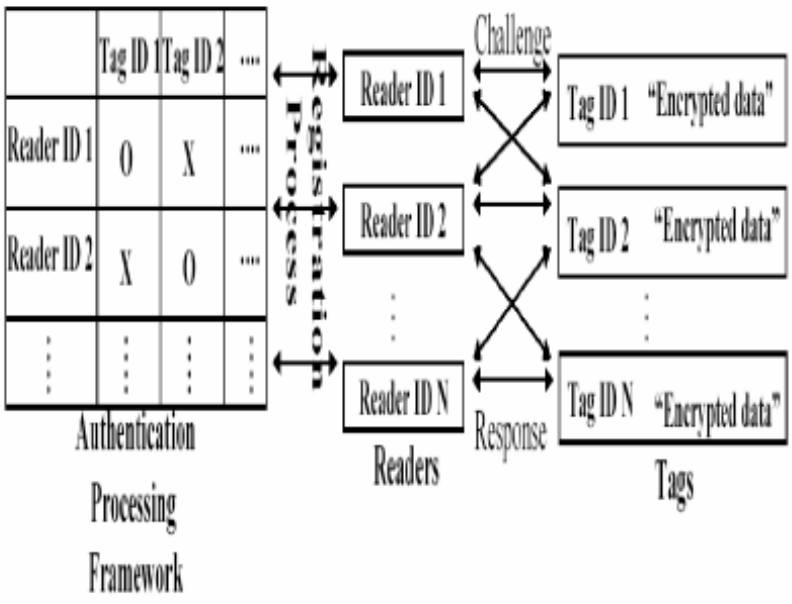


Figure 36. Registration/Access Control of Readers to the APF/Tag. From: [45]

When the reader sends a “read” command to the tag, the tag will reply with its identification number and encrypted data, this means that the data is encrypted and the registered reader with the APF will be able to get the decryption key to decrypt the encrypted data. Once the key is received, the data in the tag will be readable. In this framework, mutual authentication was carried out by the APF as it authenticates the reader and the tag [Figure 36]. The privacy of the information contained in the tag is protected as the data stored in the tag is encrypted and can only be read after the decryption key to access the information is received from the APF.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RETURN ON INVESTMENT

A. AXCESS CASE STUDY

1. Background

A study was performed by Axcess Corporation in April 2005 at a large civilian medical facility to analyze the cost effectiveness of using RFID for the location of patients, staff, and equipment in such an expansive space [46]. By comparison, the large medical facility used for the study is comparable to a large-size military treatment facility such as the Naval Medical Center in Bethesda, Maryland. The study sought to determine the viability of RFID for displacing the regular labor burden of hospital personnel inventorying, locating, and protecting hospital resources and patients. If RFID can be cost justified in a large medical facility, the business case for smaller sized medical facilities would be considered certain.

The desire was to determine if the use of RFID would save time and money in inventorying, locating, and managing the use of hospital assets. The largely manual process currently used by the facility is repetitive, redundant and time-consuming creating a frustrating, stressful, and sometimes difficult environment. Personnel have to spend the time to locate the barcode on each asset to perform a count and location inventory which is compounded by the fact the assets are in motion in and around the hospital. Assets may go missing for up to two weeks at a time creating a concern as to their whereabouts and the status of the devices and information on them along with the safety of the patients. The current system does not provide manageable custodian relationship to make sure the proper personnel are using and managing the proper assets.

The concept was to use RFID to automate tracking and inventory functions. RFID tags placed on the hospital resources would automatically transmit a signal which could be interpreted for location consideration and for inventory counting. The RFID tag ID would be linked to the data on the asset in the system providing a total inventory snapshot and enable an exceptions-based operation. The goal would be for labor hours associated with the manual bar-code surveys to be reduced and daily activities would be generated based upon the RFID tag read data on patient movements and missing assets.

The inherent benefits of the RFID system design included the ability to offer automatic protection from patients and assets leaving a room without being recognized.

2. System Considerations

Active RFID tags can be programmed to beacon at whatever beacon rate desired. Tag beacons are related to each receiver's identification for the square footage covered by the receiver and that coverage map is displayed on the computer screen with icons indicating the location zone. This receiver coverage area is engineered in size by each receiver to conform to the area to be managed. The precision of the location data is based upon the layout of the facility and the number of receivers used for the desired granularity. Receiver count directly relates to cost so there are system design cost trade-offs to be considered. Zonal size can range from as little as 50 square feet to over 4,000 square feet depending on the receiver design. Beaconing active RFID tags typically last 3 to 5 years if beaconing is set for a couple of times a day. More frequent beaconing shortens the battery life. Tags transmit a signal when battery power is getting low and replaceable battery options exist. Additionally, tags can be programmed to wake-up and transmit only when in motion so the battery is not constantly being used to re-affirm location for assets that are stationary and are not constantly transmitting.

The real advantage of RFID operation is gained when activating the tag only when it passes out of a control point such as through a doorway. This on-demand approach uses a separate activation field and devices where the tag listens for a wake-up signal from an antenna placed at the control point boundary. The boundary can be an exit door, a hallway point, or a virtual place in an open area. This activation approach provides precise "in or out" location determination as well as the direction the subject asset or individual is traveling. Only with this technique can personnel be certain that an asset has left a secured area or room. Beaconing signals alone spill over doorways and security points and prevent an application called "asset protection". Adding activation control points adds infrastructure cost to the system, however, the value of the asset being protected can be considered in the ROI calculation.

3. System Design

The system design included ten receivers on the existing local area network and fourteen “on-demand” tag activation equipment installations at doorways covering over 80,000 total square feet. RFID solutions are installed where the equipment is invisible and covert. No portals or antennas are visible which improves the aesthetic design and the security. The average location precision of a control zone was approximately 1,400 square feet within which an asset could be located within each room.

Every tagged asset beacons a signal on a regular basis to receivers which relay the tag signal to a database. As assets move between rooms or control zones, they are awakened at the doorway. The tag reports its ID and the ID of the activation doorway over the network to the database and software.

Existing access control cards could be linked through the existing personnel access control system. In this configuration, the approved check-out of an asset requires the holder to present their badge to a passive access control reader so the system can check for an authorized custodial relationship. RFID badges can be issued which provides an automatic and non-intrusive relationship check and assignment as assets and custodians move in and around the facility.

4. Software

Microsoft Windows-based desktop software was included to automatically account for and provide locations for the tagged assets and to interface to alarm equipment in the event of the loss of an asset or inappropriate location. The software and computer ran on the existing facility network. The database collected tag reads and supported inventory counts and location determination. Exception reporting for unauthorized assets and individuals leaving an assigned area included an interface into the security alarm system for automatic alarming in the event it occurred.

5. Financial Analysis

The ROI model used the most common methods of financial analysis for an IT project including the Internal Rate of Return (IRR), Net Present Value (NPV) of the savings over time, and the payback period or breakeven point. The key intangible and

variable savings item for the model was the value of protecting assets from loss or patients going astray. The value of the information on those lost assets or patients also qualifies in the intangible savings that could be gained.

The pricing of the system in the base case analysis included a total infrastructure cost of $19,000 (or $1,350 average per "control zone"). Individual RFID asset tags were priced at $15.00 each. The amortized average cost per asset per month for RFID tagging came out to be $1.00 per month per asset over an assumed 36 months. The total capital cost of the entire system including installation and software on a per tag basis came to $36.35 each. In RFID systems analysis, this measure addresses the total cost of ownership by normalizing the different architectures (i.e. passive, semi-passive) down to the average total cost per tag including all aspects of the system. The analysis returned a positive 63% internal rate of return (IRR) for the savings, a 2.2 year payback for the system, and over $22,000 in net present value savings (NPV) with the assumption of a 12% discount rate or cost of capital.

6. Summary

The financial case is justified for using RFID in a large medical facility for automatically inventorying, locating, and protecting assets that help generate savings on manpower and reducing the risk of losing an asset and patients. The financial case improves dramatically when asset protection is included especially when asset misplacement or loss is likely to be more prevalent. In some cases, the true cost of losing information on assets and personnel is incalculable. This is typical in the majority of hospitals as well as other facilities like government, educational, and enterprise installations.

B. JACOBI MEDICAL CENTER

1. Introduction

Jacobi Medical Center is one of the premier hospitals in the New York City Health and Hospitals Corporation. Jacobi employs the Misys computerized patient record (CPR) system for a variety of clinical functions including order management and clinical documentation. Jacobi also uses the Misys pharmacy, laboratory, and radiology

systems. For the past seven years, Jacobi has had a barcode system for medication administration using a McKesson robot to re-label individual medication doses [47].

2. Problem

Jacobi Medical Center had achieved good results with its barcode medication system. Despite its success, nurses were still devoting 150 minutes of each 12-hour nursing shift to medication administration tasks that consume a significant portion of the normal workday. Any automation capabilities that could reduce this burden would be helpful. The use of the barcode patient ID wristband meant that each time a nurse wanted to administer medication to a patient, he or she would have to physically lift and hold the patient's hand to wand the patient's ID barcode. This results in extra effort for the nurse and inconvenience for the patient, particularly if the patient is asleep or has an IV line in place on the wrist carrying the ID band.

3. Objective

Daniel Morreale, Chief Information Officer (CIO) at Jacobi, was convinced that the medication administration process could be improved through the use of Radio Frequency Identification (RFID) technology. He wanted to investigate the possibility of eliminating keystrokes entirely during the medication administration process using tablet PCs equipped with RFID and wireless capability. The goal would be to enable nurses to identify the patient and complete the medication administration documentation process without requiring any keystrokes that would save nursing time and minimize patient inconvenience.

4. Approach

Jacobi selected Siemens as the integration partner for this project. The hospital chose two pilot nursing units and equipped them with a wireless infrastructure. Jacobi deployed tablet PCs equipped with RFID capabilities as well as wireless access to the hospital's Misys CPR system. A small Windows script was written for the tablet PC using Visual Basic. The program performed an RFID Identification when the nurse's reader came in proximity with the patient's wristband, determined the corresponding

patient, and entered the appropriate identification and navigation commands to automatically take the nurse directly to the correct screen within the medication administration documentation program. The nurse will then wand each of the barcode labels on the individual medication doses and administer them to the patient. The Misys medication administration program would automatically document that the dosage of each medication given was appropriate based on the barcode reading. Using this system, it became feasible to perform medication administration and the associated documentation using a portable device at the bedside without requiring the nurse to make any keystrokes.

5. Results

Project expenses were reasonable. The RFID reader associated with each tablet PC cost $125. Disposable wristbands with an embedded RFID Tag cost $1.25 each. One special function printer costing $3,500 was installed in the admissions department to print the appropriate information on the patient's wristband at the time of admittance. Additional project costs included management fees paid to Siemens and one full-time IT staff member for approximately two weeks.

To measure the project's benefits, Jacobi performed a brief analysis of each nursing unit before launching the pilot study to determine the baseline level of effort required for medication administration. It took eight weeks to develop the software, identify and acquire the appropriate hardware, assemble the solution, and test it. The system was initially deployed on two nursing units and later extended to a third. Following system deployment, a repeat analysis was performed to determine potential savings.

The project team overcame the minor problems it encountered. Initially, the IT management support for the wireless network was not adequate. Later, the hospital ran out of RFID tags and had to purchase more.

Jacobi considered the RFID project a significant success. The hospital determined that approximately 25 minutes of the time is saved in the medication administration process per nurse per 12-hour shift. The ability to save time had been

established as one of the primary quantitative goals of the project. The project also succeeded in providing rapid access to patient records at the bedside. More importantly, nursing and patient satisfaction has increased significantly as indicated by the nursing staff in the pilot units insisting for the equipment to remain in place after the pilot was completed.

6. Summary

Many healthcare institutions are wondering whether radio frequency identification can play a productive role in their medication administration operations. To this point, most medical facilities have chosen barcode technology because it is more mature, less expensive and widely available. Jacobi Medical Center demonstrated that a relatively temporary, inexpensive installation project can result in RFID technology that delivers significant value. As RFID technology continues to mature, it can be anticipated to become an essential tool in helping healthcare organizations to decrease error rates while increasing staff satisfaction and constraining costs.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

A. INTRODUCTION

The promise of RFID stems in part, from the plethora of applications envisioned by the technology developers and potential users. Applications such as enhanced tracking in the supply chain, integration of inventory and logistics systems, automated monitoring of product availability and quality, control of critical infrastructure facilities, and improved security applications are propelling RFID to the market. While the efficiency-enhancing potential of RFID is high, there are differing time frames associated with the adoption of RFID. For the most part, current RFID tagging is at the container, case, or pallet level for inventory and shipping applications.

B. THESIS QUESTIONS REVIEW

1. Is the existing Navy Medicine network infrastructure capable of supporting RFID implementation?

This study initially set out to review the existing Navy Medicine network infrastructure to determine its capability to support RFID implementation. Using the information gathered from the review, the study intended to conduct research on commercially available RFID solutions successfully employed at civilian hospitals that would match the common network infrastructure used at Navy medical facilities.

Department of Defense security policies, Bureau of Medicine and Surgery guidelines, and the current information security posture precluded this study from obtaining information on network infrastructure previously coordinated during the development of the proposal for this thesis. Consequently, this question will be left unanswered; however, it may potentially be addressed in the future when the respective agencies have authorized the sharing of the needed information or the conditions of the information security situation have improved.

2. What are the requirements for the deployment of RFID within Military Treatment Facility (MTF) and what are the challenges involved?

Successful RFID implementation in the supply chain industry focused on meeting the user requirements of speed of transmission, bandwidth efficiency, reliability of the system, range, security, and cost associated with the implementation. User requirements for successfully implementing RFID technology in Navy Medicine would not be any different from that used in the supply chain industry. In some situations, such requirements for Navy Medicine implementation would even require higher percentages of speed, reliability, and range to ensure that patients and personnel can be located during emergencies. Having the readers and tags emitting only the location signals for patients and staff also provides the flexibility for hospitals to track only the location of the individuals without having medical information attached to the signal. This flexibility reduces the hospitals' burden of minimizing exposure of protected personal information in compliance with HIPAA regulations.

Despite the potential benefits of using RFID, the existing tag technology presents a number of challenges. The existence of different standards creates a potential problem for manufacturers and developers to choose between standards and develop applications that might work under one standard and not the other. The complexity of the components adds to inconsistency problems during deployment that might interfere with other medical devices used in the hospitals. Existing tag technology also features limited situational read rates and transmission conflicts along with the problem of competing standards for transmission protocols. While these challenges should be tackled as the technology moves closer to mainstream, in the interim, they will slow down the adoption process.

3. What would be the benefits associated with the implementation of RFID within Navy Medicine?

Over the years, RFID technology has proven its usefulness in many applications such as toll collection, access management and manufacturing. While its application in the hospital and healthcare environments is still very limited, results coming from the field indicate tremendous potential. Potential benefits that could be attained through the

use of RFID in Navy Medicine would include continuous real-time tracking of staff, patients and visitors throughout the hospital without infringement of personal information. This benefit would provide hospitals the ability to monitor and track unauthorized people wandering into restricted areas for better enforcement of security policies. It would also provide the medical staff a more efficient way to access a patient's medical records whenever the need arises. Navy medical facilities could save thousands of dollars by using RFID to track expensive and critical medical devices in real-time for better accounting and faster retrieval. Lastly, the ability to accurately match test specimens to the respective patients will help reduce medical errors and prevent exposing the patients to untoward medical risks.

4. What would be an ideal architectural design for the deployment of RFID?

Navy medical treatment facilities are classified into small, medium, and large hospitals. The network infrastructure for each site is funded for and equipped by the Triservice Information Management Project Office (TIMPO) from the Tricare Management Activity (TMA) funding authorization. The network infrastructure for each medical facility is also determined considering the geographical location and potential restrictions by host region or country in terms of telecommunications regulations and cabling structure. Due to network vulnerability issues and the overwhelming threat of security breaches and compromise of patient information, none of the Navy medical treatment facilities has integrated a wireless network infrastructure that would be an integral part of a RFID implementation. As such, the system infrastructure reviewed in this study would only provide potential options for RFID implementation at Navy medical treatment facilities when the leadership of Navy Medicine has deemed it appropriate to embark on full RFID deployment. Until then, an ideal architectural design for full RFID implementation may be continuously changing based on future development of the tags and readers and their ability to provide assurance against compromise of protected patient information.

5. Would the policies involved in RFID implementation hinder a successful adoption of RFID technology within Navy Medicine?

The business rules for the use of high data capacity RFID was finalized under the memorandum issued by the Under Secretary of Defense on July 30, 2004. Under this memorandum, DoD Components are tasked to immediately resource and implement the use of RFID in the operational environment in such a way that only RFID capable systems are acquired beginning in 2007.

Even though RFID has been used and implemented in most hospitals and healthcare facilities, the focus of such implementation has been on supply chain management in the form of asset tracking and inventory. Standards and policies for use of RFID in healthcare institutions particularly within the Department of Defense have not been established up to this date. Consequently, implementation of RFID technologies in Navy Medicine for personnel and patient tracking will not be affected by policy until guidelines have been determined.

C. SUMMARY

The world as we know it will be transformed by the diversification of RFID use in healthcare and its expanded adoption across industries. Experts believe that RFID technology will offer levels of convenience and efficiency in the hospital environment that are way ahead of current standards. Using this technology, hospitals can facilitate daily nursing tasks and increase the speed of identification for individual items and people that can be located and identified in wide or confined spaces.

Navy Medicine's requirements of speed in transmission, bandwidth efficiency, reliability, range, security, and cost are constant areas of improvement in the refinement of RFID components and performance. Even at the current standards levels, implementation of RFID technology at medical facilities promise major improvement in efficiency and competency in providing patient care while improving the security and quality of life for both patients and staff. The investment that will be used to install RFID capabilities can be easily recovered from the reduced medical errors and costly litigations that normally drain hospital financial resources. While RFID will not go a long way

towards directly prolonging lives, it will make such lives more comfortable and productive in a hospital environment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX - UNDER SECRETARY OF DEFENSE MEMORANDUM FOR DOD COMPONENTS, JULY 30, 2004 SUBJECT: RADIO FREQUENCY IDENTIFICATION (RFID) POLICY

MEMORANDUM FOR SECRETARIES OF THE MILIARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS, COMBATANT COMMANDS
DEPUTY UNDER SECRETARY OF DEFENSE, LOGISTICS, MATERIEL AND READINESS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS
DIRECTOR, DEFENSE PROCUREMENT AND ACQUISITION POLICY
DIRECTOR, SMALL AND DISADVANTAGED BUSINESS UTILIZATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Radio Frequency Identification (RFID) Policy

In my capacity as the Defense Logistics Executive (DLE), this memorandum issues the policy for implementing Radio Frequency Identification (RFID) across the Department of Defense (DoD). This policy finalizes the business rules for the use of high data capacity active RFID (Attachment 1) and finalizes the business rules for the implementation of passive RFID and the use of Electronic Product Code (EPC) interoperable tags and prescribes the implementation approach for DoD suppliers/vendors to apply passive RFID tags. This policy memorandum applies to the Office of the Secretary Defense (OSD); the Military Departments, the Joint Chiefs of Staff and the Joint Staff; the Combatant Commands; the Inspector General of the Department of Defense; the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as the "DoD Components"). An internal implementation strategy for DoD Components to read and apply passive RFID will be issued in a separate Defense Logistics Executive (DLE) decision memorandum. This policy supersedes two previous issuances of policy dated October 2, 2003 and February 20, 2004.

DoD Components will immediately resource and implement the use of high data capacity active RFID in the DoD operational environment. Attachment 1 outlines the detailed guidance on active tagging. DoD Components must ensure that all consolidated shipments moving to, from, or between overseas locations are tagged, including

retrograde, and must expand the active RFID infrastructure to provide global intransit visibility. In order to take advantage of global RFID infrastructure not within the DoD's control, the DoD Logistics Automatic Identification Technology Office will assess the ability to leverage any compatible active RFID commercial infrastructure that commercial entities may establish. This should not b viewed as direction to commercial carriers and port operators to establish an active RFID infrastructure.

Attachment 2 contains the detailed guidance on implementation of passive RFID capability within the DoD supply chain as well as the data constructs for the tags. DoD will use and require its suppliers to use EPC Class 0 and Class 1 tags, readers, and complementary devices. DoD will migrate to the next generation tag (UHF Gen 2) and supporting technology. When the specification for UHF Gen 2 is finalized, the Department will announce a transition plan to this technology, but we expect use of EPC Class 0 and Class 1 technology for approximately two years.

Radio Frequency Identification will be a mandatory DoD requirement on solicitations issued on or after October 1, 2004 for delivery of materiel on or after January 1, 2005 in accordance with the supplier implementation plan at Attachment 3. Contracts with DoD shall require that passive RFID tags be applied to the case, pallet and item packaging for unique identification (UID) items in accordance with Attachment 3. The Defense Logistics Board (DLB) will review the internal implementation plan, benefits, compliance requirements, and requisite budget requirements annually based on an assessment of the implementation to date. This review will include an updated analysis of implementation success as well as provide guidance for expansion of RFID capabilities into additional applications and supply chain functional processes. A DLE decision memorandum will provide funding guidance for DoD Component implementation.

In order for the DoD Component to meet the requirements of this policy, we have developed a Department-wide RFID Concept of Operations (CONOPS) to outline the transformational role of RFID technology in DoD logistics and to articulate the specific uses of both active and passive RFID throughout the DoD supply chain. Components will prepare a supporting RFID implementation plan that encompasses both active and passive RFID technology in a cohesive environment to support the DoD vision. Active RFID implementation plans are already due and an update to include passive RFID implementations is due to the ADUSD (SCI) by October 29, 2004 to ensure total interoperability and standardized implementation throughout the Department.

To support the purchase of passive RFID technology and leverage the purchasing power of the Department, the Army's Program Executive Office Enterprise Information Systems (PEO EIS) continues development of a multi-vendor contract mechanism to procure EPC technology. This contract will include competitive vendors providing RFID equipment/infrastructure in accordance with current published EPC specifications (Class 0 and Class1) and, when published, specifications for UHF Gen 2.

To institutionalize RFID as a standard way of doing business, this policy will be incorporated into the next update of the DoD Supply Chain Materiel Management Regulation (DoD 4140.1-R), the Defense Transportation Regulation (DoD 4500.9-R) and the Military Standard 129. Likewise, DoD Components will incorporate this policy into Service/Agency level publications as well as Component strategies to achieve compliance with the DoD Business Enterprise Architecture – Logistics (BEA- LOG).

The following policy also applies to take full advantage of the inherent life cycle management efficiencies of this technology. Beginning in FY 2007 and beyond – only RFID capable AIT peripherals (e.g. optical scanners, printers used for shipping labels) will be acquired when these peripherals support RFID-capable business processes. Beginning in FY 2007 and beyond – logistics automated information systems (AISs) involved in receiving, shipping, and inventory management will use RFID to perform business transactions, where possible, and AIS funding will hinge on compliance with this policy.

Managers of all major logistics systems modernization programs will update appropriate program documentation to include the requirement for RFID capabilities as part of the system operational deployment in conformance with the business rules and initial timeline set forth in this policy. Managers of major acquisition programs will update programs as required to include the requirement for RFID capabilities where applicable. The DLB will review these requirements prior to FY 2007 implementation.

We will continue to partner with your staffs as well as our suppliers on this critical initiative. RFID remains part of the larger suite of AIT technologies and the Department will leverage all of these technologies, where appropriate in the supply chain, to improve our ability to support the warfighter. However, an RFID-capable DoD supply chain is a critical element of Defense Transformation and will provide a key enabler for the asset visibility support down to the last tactical mile that is needed by our warfighters. Your continued efforts are vital to our success in meeting this requirement. For further information, please refer to our website at www.dodrfid.org.

/S/
Michael W. Wynne
Acting

Attachments:
As stated

THIS PAGE INTENTIONALLY LEFT BLANK

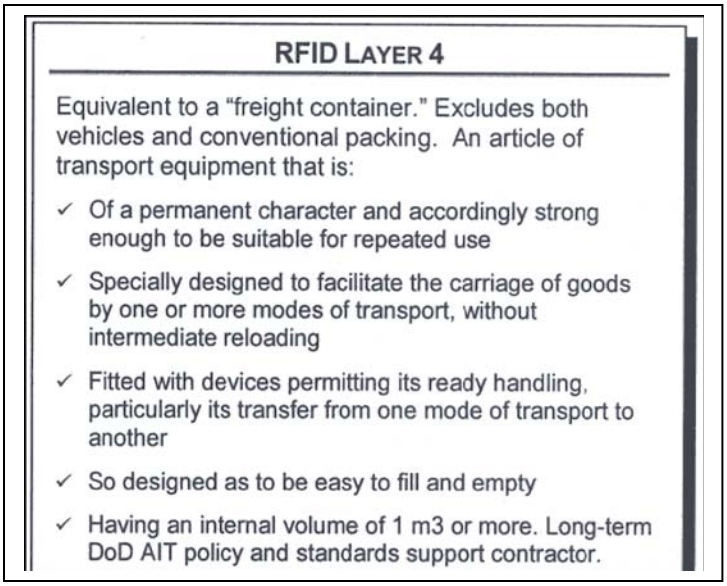
Business Rules for Active RFID Technology in the DoD

1.1 Overview

Active Radio Frequency Identification (RFID) tags used in DoD are data rich and allow low-level RF signals to be received by the tag, and the tag can generate high-level signals back to the reader/interrogator. Active RFID tags can hold relatively large amounts of data, are continuously powered, and are normally used when a longer tag read distance is desired.

The DoD Logistics Automatic Identification Technology (LOG-AIT) Office is the DoD focal point for coordinating overarching guidance for the use of AIT within DoD. The Program Executive Office, Enterprise Information Systems (PEO EIS), Product Manager -Automatic Identification Technology (PM-AIT) Office is the DoD procurement activity for AIT equipment (to include RFID equipment and infrastructure) and maintains a standing contract for equipment integration, installation, and maintenance. The Defense Logistics Agency (DLA) is the procurement activity and single manager for active RFID tags. Users will coordinate RFID equipment/infrastructure procurement through the PM-AIT Office and tag procurement from DLA to ensure interoperability and compliance with this policy.

The following business rules are applicable to all DoD Components. They support asset visibility and improved logistic business processes throughout the DoD logistics enterprise. These rules specifically apply to DoD cargo shipped outside the Continental United States (OCONUS), however, organizations are encouraged to employ the use of active RFID technology for Intra-Continental United States (CONUS) shipments to support normal operations or for training.



1.2 Active RFID Business Rules

1.2.1 Sustainment/Retrograde Cargo

All consolidated sustainment or retrograde shipments (RFID Layer 4 freight containers (e.g., 20 or 40 foot sea vans, large engine containers and 463L air pallets) of DoD cargo being shipped OCONUS must have active, data-rich RFID tags written at the point of origin for all activities (including vendors) stuffing containers or building air pallets. Content level detail will be provided in accordance with current DoD RFID tag data specifications. Containers and pallets reconfigured during transit must have the RFID tag data updated by the organization making the change to accurately reflect current contents.

CONTENT LEVEL DETAIL

Content level detail comprises two components: (1) Asset Level Detail (i.e. data elements that describe the asset) and (2) Content Level Detail - data elements that minimally identify each level of a complete shipment entity (a single shipment unit or a consolidated shipment).

1. Asset Level Detail. The minimum data elements required to describe the physical characteristics of a single asset, and the characteristics that identify that asset.

- ✓ National Stock Number (NSN)
- ✓ Nomenclature/Description Model Number
- ✓ Unit Price (U/P)
- ✓ Condition Code
- ✓ Serial Number / Bumper Number
- ✓ Serial Number Enterprise Identifier (if UID eligible)
- ✓ Part Number (if UID eligible, as applicable)
- ✓ Item Weight
- ✓ Item Cube
- ✓ Line Item Number (LIN)/Package Identification (PKGID)
- ✓ Ammunition Lot Number
- ✓ Department of Defense Identification Code (DODIC)
- ✓ Hazardous Cargo Descriptor Codes (to include ammo/ hazardous materiel).

2. Content Level Detail Visibility for Each Shipment Unit. The most basic transportation entity is a single box or unpacked item governed by a shipment unit identifier. The data elements are contained in the requisition document, Transportation Control and Movement Document (TCMD), commercial carrier transaction, and the Consolidated Shipment Information transaction that describes the shipment and shipment movement characteristics. Minimum data elements necessary to provide content level visibility for each shipment unit are:

- ✓ Requisition Document Number
- ✓ Required Delivery Date (RDD) or expedited shipment and handling codes
- ✓ Project Code
- ✓ Asset (item) Quantity
- ✓ Unit of Issue (U/I)
- ✓ 'From' Routing Indicator Code (RIC) (for DOD shipments)
- ✓ Inventory Control Point (ICP)
- ✓ RIC (for contractor/vendor shipments)
- ✓ Shipment Transportation Control Number (TCN) – for single shipment unit
- ✓ Intermediate TCN – for a multi-level consolidated shipment
- ✓ Conveyance (lead) TCN – for a consolidated shipment
- ✓ Commercial Carrier Shipment Tracking Identifier
- ✓ Transportation Priority
- ✓ Sender (Consignor) DODAAC/CAGE Code
- ✓ Ship Date
- ✓ Port of Embarkation (POE) Code
- ✓ Port of Debarkation (POD) Code
- ✓ Shipment Total Pieces
- ✓ Shipment Total Weight
- ✓ Shipment Total Cube
- ✓ Oversize Length/Width/Height
- ✓ Receiver (Consignee) DODAAC
- ✓ Commodity Class
- ✓ Commodity Code (air/water)
- ✓ Special Handling Code (air/water)
- ✓ Water Type Cargo Code
- ✓ Net Explosive Weight (NEW)
- ✓ Unit Identification Code (UIC)
- ✓ Unit Line Number (ULN)
- ✓ Operation/Exercise Name
- ✓ Hazardous Material (HAZMAT) Shipping Characteristics: United Nations Identification Number (UNID), Class or Division Number, Package Group, Compatibility Group.

1.2.2 Unit Movement Equipment and Cargo

All RFID Layer 4 freight containers and palletized unit move shipments being shipped OCONUS, as well as all major organizational equipment, must have active data-rich RFID tags written and applied at the point of origin for all activities (including vendors) stuffing containers or building air pallets. Content level detail will be provided in accordance with current DoD RFID tag data standards. Self -deploying aircraft and ships are exempt.

1.2.3 Ammunition Shipments
All RFID Layer 4 freight containers and palletized ammunition shipments being shipped OCONUS must have active data-rich RFID tags written with content level detail. Tags will be applied at the point of origin by all activities (including vendors) that stuff containers or build air pallets in accordance with current DoD RFID tag data specifications. Containers and pallets reconfigured during transit must have the RFID tag data updated to accurately reflect current contents by the organization making the change.

1.2.4 Pre-positioned Materiel and Supplies
All RFID Layer 4 freight containers and palletized pre-positioned stocks or War Reserve Materiel as well as all major organizational equipment must have active data-rich RFID tags written with content level detail and applied at the point of origin by all activities, including vendors. Execution for current afloat assets will be completed during normal maintenance cycle, reconstitution/reset, or sooner as required.

1.2.5 RFID Infrastructure
USTRANSCOM will ensure that designated strategic CONUS and OCONUS aerial ports and seaports (including commercial ports) supporting Operation Plans (OPLANs) and military operations have RFID equipment (interrogators, write stations, tags, brackets) with read and/or write capability to meet Combatant Commander requirements for asset visibility. Military and commercial ports will be instrumented with fixed or mobile RFID capability based on volume of activity and duration of the requirement at the port. Military Departments and Combat Support Agencies will ensure sufficient RFID infrastructure and equipment (interrogators, write stations, tags, and brackets) are appropriately positioned to support Combatant Commander requirements for asset visibility. As above, military and commercial ports will be instrumented with fixed or mobile RFID capability based on volume of activity and duration of the requirement at the port.
To ensure that users take maximum advantage of inherent efficiencies provided by this technology, RFID capability will be operational at logistic nodes and integrated into existing and future logistics automated information systems. RFID recorded events will become automatic transactions of record. Geographical Combatant Commanders may direct Service Components/Combat Support Agencies to acquire, operate, and maintain additional theater supporting RFID infrastructure to meet changing theater operations. As a general rule, an organization responsible for port or logistics node operation is also responsible for installing, operating, and maintaining appropriate RFID capability. Additionally, when responsibility for operating a specific port or node changes (e.g., aerial port operations change from strategic to operational), the losing activity is responsible for coordinating with the gaining activity to ensure RFID capability continues without interruption.

1.3 RFID Funding
The cost of implementing and operating RFID technology is considered a normal cost of transportation and logistics and as such should be funded through routine Operations and Maintenance or Working Capital Fund processes. It is the responsibility of the activity at

which containers, consolidated shipments, unit move items, or air pallets are built or reconfigured to procure and operate sufficient quantities of RFID equipment to support the operations. Working Capital Fund activities providing this support will use the most current DoD guidance in determining whether operating cost authority or capital investment program authority will be used to procure the required RFID equipment. If the originating activity of the Layer 4 container/consolidated air pallet is a vendor location, it is the responsibility of the procuring Service/ Agency to arrange for the vendor to apply active tags, either by obtaining sufficient RFID equipment to provide the vendor to meet the requirement, or requiring the vendor as a term of the contract to obtain necessary equipment to meet the DoD requirement. Additionally, Combatant Commanders are responsible for coordinating with their Service Components to ensure adequate enroute RFID infrastructure is acquired and operating at key logistics nodes.

1.4 RFID Tag Return

The DLA automated wholesale management system will provide tags through existing supply channels. The DoD Item Manager for the active RFID tags (NSN 6350-01-495-3040) is the Defense Supply Center Philadelphia, Inventory Control Point, Routing Identifier Code S9I. Only new Condition Code A tags will be sold to customers. All returned tags that are serviceable after refurbishment will be received into wholesale inventory as Condition Code B and will be available as free issue from the DLA Defense Distribution Center (DDC) when they are placed on a pallet or container by DDC. This will spread the savings across the DoD Community of active tag users. When DDC requisitions tags, Condition Code B tags will be issued first. If there are no Condition Code B tags available for issue to the DDC, the DDC will pay the standard price for Condition Code A tags. Activities are encouraged to use the Defense Logistics Management Supplement Materiel Returns Program (MRP) to return tags no longer required and receive reimbursement for packaging, crating, handling, and transportation (PCH&T) costs. Excess tags sent back without MRP transactions will not result in PCH&T reimbursement to the customer. The PCH&T 'reimbursement incentive for tags received with MRP transactions will result in reduced costs and savings to DoD from reusing the Condition Code B tags. The Military Services, other requisitioners, and users may opt to establish their own retail operation for used tags and incur the cost of refurbishment themselves.

1.5 RFID Tag Formats

The DoD LOG-AIT Office is responsible for coordinating, establishing, and maintaining RFID tag formats at the data element level. RFID tagging procedures require active data-rich RFID tags be written with content level detail in accordance with approved formats RF-Tag Data Format Specification, Version 2.0, the current version. RFID tag data files will be forwarded to the regional in-transit visibility (ITV) server(s) in accordance with established DoD data timeliness guidelines published in the current versions of the DoD 4500.9-R, Defense Transportation Regulation and Joint Publication 4-01.4, Joint Tactics, Techniques, and Procedures for Joint Theater Distribution. RF Tag data is further transmitted to the Global Transportation Network (GTN) and other global asset visibility systems as appropriate. This tag data flow will be analyzed in the future as part of the DPO architecture. RF tag formats will be identified in the current version of DoD

4500.9-R, Defense Transportation Regulation, and the format requirements will be published in MIL STD 129, DoD Standard Practice for Military Marking for Shipment and Storage. It is the intent of the Department to incorporate all RFID tag formats and usage standards into a DoD RFID manual.

1.6 RFID I TV Server Management

The PM-AIT Office will manage the RFID ITV servers. All DoD Component operated RFID interrogators will forward their data to the ITV servers maintained by PM-AIT. This will enable the PM-AIT Office to program for funding and provide a centralized management structure for the regional ITV servers, including the I TV server on the Secret Internet Protocol Router Network (SIPRNET). PM-AIT is responsible for ensuring that ITV system performance and information assurance requirements are in accordance with DODD 8500.1, Information Assurance (IA), and DODI 8500.2, Information Assurance (IA) Implementation. The Non-classified Internet Protocol Router Network (NIPRNET)-based ITV servers must be interoperable with GTN, GTN 21, Joint Total Asset Visibility, and Integrated Data Environment, and other DoD logistics systems as determined by the PM-AIT Office and the user representative(s). The SIPRNET-based ITV server must interoperate with the Global Combat Support System, Global Command and Control System, and other classified systems as determined by PM-AIT and the User Representative(s). PM-AIT is responsible for maintaining the accreditation and net worthiness certification of all ITV servers.

1.7 Wireless Encryption Requirements

Per the DoD Wireless Policy (DODD 8100.2), encryption requirements do not apply to the detection segment of a personal electronic device (PED) e.g., the laser used in optical storage media; between a barcode and a scanner head; or Radio Frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator.

1.8 Frequency Spectrum Management

PM-AIT office will continue to assist DoD Components in frequency management issues related to active RFID tags and equipment purchased under the DoD RFID contracts by PM-AIT.

RFID tags that meet the technical specifications of 47 CFR 15 of the CC's Rules and Regulations for Non-Licensed Devices, i.e. Part 15, must accept and may not cause electromagnetic interference to any other federal or civil RF device. 47 CFR 15 only applies to use of these devices within CONUS and other US Possessions. DoD components will forward requests for frequency allocation approval via command channels to the cognizant military frequency management office to ensure that RFID tags comply with us national and OCONUS host-nation spectrum management policies. RFID tags and infrastructure may require electromagnetic compatibility analysis to quantify the mutual effects of RFID devices within all intended operational environments, (e.g. Hazards of Electromagnetic Radiation to Ordnance (HERO) and Hazards of Electromagnetic Radiation to Fuel (HERF).

Business Rules for Passive RFID Technology in the DoD

2.1 Overview

Passive Radio Frequency Identification (RFID) tags reflect energy from the reader/interrogator or receive and temporarily store a small amount of energy from the reader/interrogator signal in order to generate the tag response. Passive RFID requires strong RF signals from the reader/interrogator, while the RF signal strength returned from the tag is constrained to low levels by the limited energy. This low signal strength equates to a shorter range for passive tags than for active tags. The DoD approved frequency range for passive RFID implementation is UHF 860-960 MHz. The DoD Logistics Automatic Identification Technology (LOG-AIT) Office is the DoD focal point for coordinating overarching guidance for the use of AIT within DoD. The Program Executive Office, Enterprise Information Systems (PEG EIS), Product Manager-Automatic Identification Technology (PM-AIT) Office is the DoD procurement activity for AIT equipment (to include RFID equipment and infrastructure) and will establish a standing contract for equipment installation and maintenance. Beginning in FY 2007, only RFID capable AIT peripherals (e.g. optical scanners and printers used for shipping labels) will be acquired when those peripherals support RFID-capable business processes. Beginning in FY 2007, logistics automated information systems (AISs) involved in receiving, shipping, and inventory management will use RFID to perform business transactions, where appropriate. AIS funding will hinge on compliance with this policy. The Defense Logistics Board (DLB) will review these requirements prior to FY 2007 implementation.

2.2 Passive RFID Business Rules

The following prescribes the business rules for the application of passive RFID technology at the case, pallet, and item packaging (unit pack) for Unique Identification (UID) items on shipments to and within DoD. These rules are in addition to the UID requirement for data element identification of DoD tangible assets using 2D data matrix symbology marking on the item itself. To facilitate the use of RFID events as transactions of record, the DoD has embraced the use of Electronic Product Code (EPC) tag data constructs, as well as DoD tag data constructs, in a supporting DoD data environment. As the available EPC technology matures, the intent is to expand the use of passive RFID applications to encompass individual item tagging.

2.3 Definitions:

The following definitions apply to passive RFID technology and tags in support of the DoD requirement to mark/tag materiel shipments to DoD activities in accordance with this policy (Figure 1 depicts the definitions graphically):

> **EPC Technology**: Passive RFID technology (readers, tags, etc.) that is built to the most current published EPCglobal. Class O and Class 1 specifications and that meets interoperability test requirements as prescribed by EPCglobal. EPC Technology will include Ultra High Frequency Generation 2 (UHF Gen 2) when this specification is approved and published by EPCglobal.

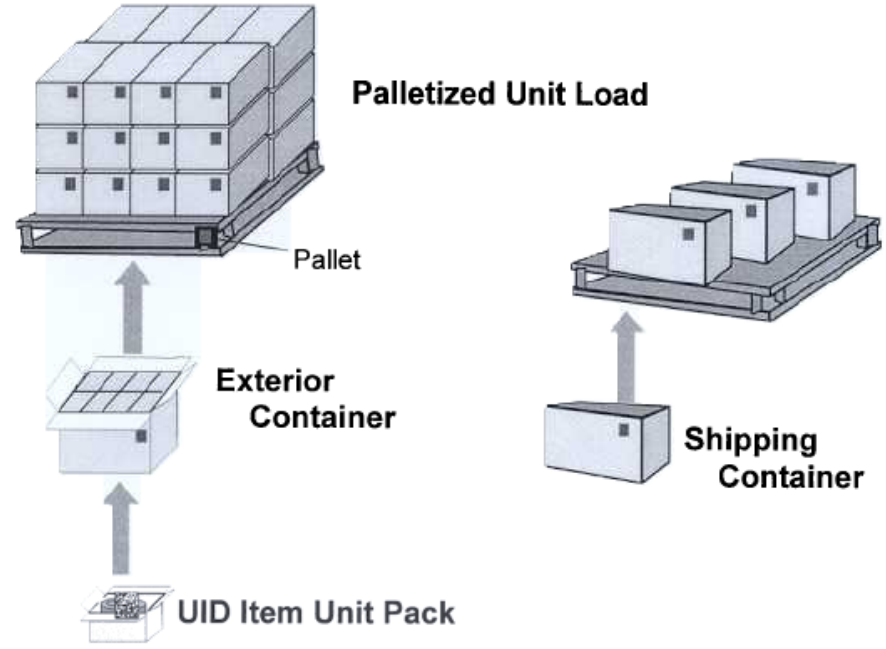
Unit Pack: A MIL-STD-129 defined unit pack specifically, the first tie, wrap, or container applied to a single item, or to a group of items, of a single stock number preserved or unpreserved which constitutes a complete or identifiable package.

Case (either an exterior container within a palletized unit load or an individual shipping container):

- Exterior Container: A MIL-STD-129 defined container, bundle, or assembly that is sufficient by reason of material, design, and construction to protect unit packs and intermediate containers and their contents during shipment and storage. It can be a unit pack or a container with a combination of unit packs or intermediate containers.
An exterior container mayor may not be used as a shipping container.
- Shipping Container: A MIL-STD-129 defined exterior container which meets carrier regulations and is of sufficient strength, by reason of material, design, and construction, to be shipped safely without further packing (e.g., wooden boxes or crates, fiber and metal drums, and corrugated and solid fiberboard boxes).

Pallet (palletized unit load): A MIL-STD-129 defined quantity of items, packed or unpacked, arranged on a pallet in a specified manner and secured, strapped, or fastened on the pallet so that the whole palletized load is handled as a single unit. A palletized or skidded load is not considered to be a shipping container.

Figure 1



2.4 Case, Palletized Unit Load, UID Item Packaging Tagging/Marking
DoD sites where materiel is associated into cases or pallets will tag the materiel and supplies at that site with an appropriate passive RFID tag prior to further trans-shipment to follow-on consignees. The Defense Logistics Agency has committed to enabling the strategic distribution centers at Defense Distribution San Joaquin, CA (DDJC) and Defense Distribution Susquehanna, PA (DDSP) with passive RFID capability by January 1, 2005.
Per the schedule outlined in Attachment 3 of this memo, case, pallet, and item packaging (unit pack) for Unique Identification (UID) items will be tagged at the point of origin (including vendors) with passive RFID tags, except for the bulk commodities listed in Section 2.4.1. If the unit pack for urn items is also the case, only one RFID tag will be attached to the container.

2.4.1 Bulk commodities not included
The following bulk commodities are defined as those that are shipped in rail tank cars, tanker trucks, trailers, other bulk wheeled conveyances, or pipelines.

- Sand
- Gravel
- Bulk liquids (water, chemicals, or petroleum products)
- Ready-mix concrete or similar construction materials
- Coal or combustibles such as firewood
- Agricultural products -seeds, grains, animal feeds, and the like

2.4.2 Contract/Solicitation Requirements
Per the schedule outlined in Attachment 3 of this memo, new solicitations for materiel issued after October 1, 2004, for delivery after January 1, 2005, will contain a requirement for passive RFID tagging at the case (exterior container within a palletized unit load or shipping container), pallet (palletized unit load), and the urn item packaging level of shipment in accordance with the appropriate interim/final Defense Federal Acquisition Regulation Supplement (DFARS) Rule/Clause or MIL-STD-129 as appropriate.

2.5 Passive UHF RFID Tag Specifications
The DoD approved frequency range for the tags is 860-960 MHz with a minimum read range of three meters. Until the EPC UHF Gen 2 tag specification is published and quantities of UHF Gen 2 items are available for widespread use, the DoD will accept the following EPC tags:

- Class 0 64-bit read-only
- Class 1 64-bit read-write
- Class 0 96-bit read-only
- Class 1 96-bit read-write

The above listed tags will be utilized for initial shipments from suppliers in compliance with appropriate contractual requirements to tag items shipped to DoD receiving points commencing January 1, 2005.
When the UHF Gen 2 EPC technology is approved and has completed any required compliance and/or interoperability testing, the DoD will establish firm tag acceptance

expiration dates (sunset dates) for EPC Version 1 (class 0 and 1) tags and will accept only UHF Gen 2 EPC tags thereafter. The DoD goal is to migrate to use of an open standard UHF Gen 2 EPC tag, Class 1 or higher, that will support DoD end-to-end supply chain integration.

Anticipated Passive EPC Version 1 Tag sunset dates for suppliers shipping to DoD:

- Class O -64 bit: At a minimum, 2 years from the publication of the specification for UHF Gen 2- subject to the availability and product maturity of this technology (i.e., UHF Gen 2).
- Class 1 -64 bit: At a minimum, 6 months from the general commercial availability and product maturity of Class 1 96 bit tags.

- Class O and Class 1 -96 bit: At a minimum, 2 years from the publication of the specification for UHF Gen 2 -subject to the availability and product maturity of this technology (i.e., UHF Gen 2).

NOTE: non will establish he tag expiration (sunset) dates and implementation dates for migration to UHF Gen 2.

As outlined below, suppliers to DoD must encode an approved tag using either a DoD tag data construct or an EPC tag data construct. Suppliers that choose to employ the DoD tag construct will use the Commercial and Government Entity (CAGE) code previously assigned to them and encode the tags per the rules that follow. Suppliers that are EPCglobalTM subscribers and possess a unique EPC manager number may choose to use the EPC tag data construct to encode tags per the rules that follow. Suppliers must ensure that each tag identification is unique.

Passive UHF RFID Tag Specifications

Class	User Memory Size (bits)	Origin	Encoding	Tag Data Constructs
0	64	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
0	64	Supplier	DoD	DoD Tag Construct
1	64	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
1	64	Supplier	DoD	DoD Tag Construct
0	96	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
0	96	Supplier	DoD	DoD Tag Construct
1	96	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
1	96	Supplier	DoD	DoD Tag Construct
1	96	DoD	DoD	DoD Tag Construct

2.5.1 Passive UHF RFID Tag Data Structure Requirements – SUPPLIERS SHIPPING TO DoD – EPCglobal™ Subscribers using an EPCglobal™ tag data construct

Tag Requirement	EPC Data Construct	When Used
UID Unit Pack	SGTIN	On item packaging for items meeting the DoD criteria for assignment of UID where a serial number is used to augment a GTIN which is used for the unique identification of trade items worldwide within the UCC.EAN System.
	GRAI	On item packaging for items meeting the DoD criteria for assignment of UID (reusable package or transport equipment of specific or certain value).
	GIAI	On item packaging for items meeting the DoD criteria for assignment of UID (used to uniquely identify an entity that is part of the fixed inventory of a company – GIAI can be used to identify any fixed asset of an organization).
Case, Pallet	SGTIN	Items shipped as either pure case, or pallet (see above)
	SSCC	Items shipped as either pure or mixed case, pallet, (SSCC can be used by all parties in the supply chain as a reference number to the relevant information held in computer database or file).

Layout for 64 Bit EPCglobal™ Data Constructs

Tag Type	Header	Filter Value	Company Prefix	Item Reference	Serial Number
SGTIN	2	3	14	20	25
Tag Type	Header	Filter Value	Company Prefix	Asset Type	Serial Number
GRAI	8	3	14	20	19
Tag Type	Header	Filter Value	Company Prefix	Individual Asset Reference	
GIAI	8	3	14	39	
Tag Type	Header	Filter Value	Company Prefix	Serial Reference	
SSCC	8	3	14	39	

Layout for 96 Bit EPCglobal™ Data Constructs

Tag Type	Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
SGTIN	8	3	3	20-40	24-4	38
Tag Type	Header	Filter Value	Partition	Company Prefix	Asset Type	Serial Number
GRAI	8	3	3	20-40	24-4	38
Tag Type	Header	Filter Value	Partition	Company Prefix	Individual Asset Reference	
GIAI	8	3	3	20-40	62-42	
Tag Type	Header	Filter Value	Partition	Company Prefix	Serial Reference	Unallocated
SSCC	8	3	3	20-40	37-17	25

2.5.2 Passive UHF RFID Tag Data Structure Requirements – SUPPLIERS SHIPPING TO DoD – non-EPCglobal™ Subscribers using the DoD tag data construct

Class 0 – 64 bit tags and Class 1 – 64 bit tags

Tag Requirement	Data Construct	When Used
UID Unit Pack	DoD Construct	On item packaging for items meeting the DoD criteria for assignment of UID
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

DoD 64-bit data construct – 64 bits total user memory on tag

Header	Filter	CAGE Code	Serial Number
8 bits	2 bits	30 bits	24 bits

Fields:

- **Header** -specifies that the tag data is encoded as a DoD 64-bit tag construct, use binary number 1100 1110.
- **Filter** -identifies a pallet, case, or urn item associated with tag, represented in binary number format using the following values:
  - 00 = pallet

- 01 = case
- 10 = UID item
- 11 = reserved for future use

- **CAGE** -identifies the supplier and ensures uniqueness of serial number across all suppliers -represented in ASCII format. (see User's Guide for details of encoding this field).
- **Serial Number** -uniquely identifies up to 224 = 16,777,216 tagged items, represented in binary number format.

Sample binary encoding of the fields of a 64 bit Class 1 tag on a case shipped from DoD supplier

Header (DoD construct)	1100 1110
Filter (Case)	01
CAGE (1D381)	11 0001 00 0100 11 0011 11 1000 11 0001
Serial Number (16,522,293)	1111 1100 0001 1100 0011 0101

Complete content string of the above encoded sample tag is as follows:

1100111001110001000100111 0011111000110001111111000001110000010101

Class 0 – 96 bit tags and Class 1 – 96 bit tags

Tag Requirement	Data Construct	When Used
UID Unit Pack	DoD Construct	On item packaging for items meeting the DoD criteria for assignment of UID
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

DoD 96-Bit Data Construct – 96 bits total user memory on tag

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields:

- **Header** -specifies that the tag data is encoded as a DoD 96-bit tag construct, use binary number 1100 1111
- **Filter** -identifies a pallet, case, or urn item associated with tag, represented

in binary number format using the following values:

- 0000 = pallet
- 0001 = case
- 0010 = urn item
- all other combinations = reserved for future use.

- **DODAAC/CAGE** -identifies the supplier and ensures uniqueness of serial number across all suppliers -represented in ASCII format. (see User's Guide for details of encoding this field).
- **Serial Number** -uniquely identifies up to 236 = 68,719,476,736 tagged items, represented in binary number format.

2.5.3 Passive UHF RFID Tag Data Structure Requirements -DoD RECEIVING POINTS SHIPPING ITEMS DOWN THE SUPPL y CHAIN TO DoD CUSTOMERS

NOTE: DoD initial implementations will use currently available 64-bit tags but should transition to 96-bit tags as soon as practicable, but not later than January I, 2005.

Class 1 – 96 bit tags

Original Tag Requirement	DoD Shipping Tag Data Construct	When Used
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

DoD 96-Bit Data Construct - 96 bits total user memory on tag

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields:

- **Header** -specifies that the tag data is encoded as a DoD 96-bit tag construct, use binary number 1100 1111
- **Filter** -identifies a pallet, case, or urn item associated with tag, represented in binary number format using the following values:
  - 0000 = pallet
  - 0001 = case
  - 0010 = urn item
  - all other combinations = reserved for future use
- **DODAAC/CAGE** -identifies the supplier, insures uniqueness of serial number across all suppliers, represented in ASCII format

- **Serial Number** -uniquely identifies up to 236 = 68,719,476,736 tagged items, represented in binary number format

Sample binary encoding of the fields of a 96 bit Class 1 tag on a case shipped from DoD internal supply node

Header (DoD construct)	1100 1111
Filter (Case)	0001
DODAAC (ZA18D3)	0101 1010 0100 0001 0011 0001 0011 1000 0100 0100 0011 0011
Serial Number (12,345,678,901)	0010 1101 1111 1101 1100 0001 1100 0011 0101

Complete content string of the above encoded sample tag is as follows:

110011110001010110100100000100110001001110000100010000110011001011011111110111000001110000110101

NOTES:

1. Specific tag orientation and location, as well as physical mounting requirements will be addressed in MIL-STD 129.
2. Advance Ship Notices (ASNs) will be required as specified in contracts in accordance with the appropriate DFARS Rule/clause.
3. It is the intent of the Department to incorporate all RFID tag formats and usage standards into a DoD RFID manual.

2.6 Electronic Data Interchange (EDI) Information

To effectively utilize RFID events to generate transactions of record in DoD logistics systems, RFID tag data with the associated material information must be resident in the DoD data environment so that information systems can access this data at each RFID event (i.e., tag read).

The DoD will require commercial suppliers to provide standard Ship Notice/Manifest Transaction Set (856) transactions in accordance with the Federal Implementation Convention (IC) via approved electronic transmission methods (EDI, web-based, or user defined format) for all shipments in accordance with the applicable DF ARS Rule via Wide Area Workflow (W A WF). Internal DoD sites/locations and shippers will use the EDI IC 856S or 856A, as applicable.

The transaction sets enable the sender to describe the contents and configuration of a shipment in various levels of detail and provide an ordered flexibility to convey information. The Federal IC 856 and DoD IC 856S and 856A transaction sets will be modified by the appropriate DoD controlling agencies to ensure the transactions can be used to list the contents for each piece of a shipment of goods as well as additional

information relating to the shipment such as: order information, product description to include the item count in the shipment piece and item UID information, physical characteristics, type of packaging to include container nesting levels within the shipment, marking to include the shipment piece number and RFID tracking number, carrier information, and configuration of goods within the transportation equipment. The DoD will also accept the submission of web-based ASN transactions as well as User-Defined-Format (UDF) ASN files. The following required ASN transactions will facilitate this use of RFID events.

Required ASN Transactions

RFID Event Type	RFID Tag Data Construct	ASN Required	ASN Type
Shipment from Supplier	SGTIN	Yes	856/WAWF Web or UDF
	GRAI	Yes	856/WAWF Web or UDF
	GIAI	Yes	856/WAWF Web or UDF
	SSCC	Yes	856/WAWF Web or UDF
	Manufacturer Encoded Tag Serialization	Yes	856/WAWF Web or UDF
	DoD Construct	Yes	856/WAWF Web or UDF
DoD Shipper to DoD customer	Manufacturer Encoded Tag Serialization	Yes	856S or 856A via DAAS
	DoD Construct	Yes	856S or 856A via DAAS

2.7 RFID Funding

The cost of implementing and operating RFID technology is considered a normal cost of transportation and logistics and as such should be funded through routine Operations and Maintenance, Working Capital Fund, or Capital Investment processes. It is the responsibility of the DoD activity at which cases or palletized unit loads are built to procure and operate sufficient quantities of passive RFID equipment (interrogators/readers, write stations, tags, etc.) to support required operations. It is the responsibility of the activity at which cases or palletized unit loads are received, (i.e., activity where the "supply" receipt is processed) to procure and operate sufficient quantities of passive RFID equipment (interrogators/readers) to support receiving operations. Working Capital Fund activities providing this support will use the most current DoD guidance in determining whether operating cost authority or capital investment program authority will be used to procure the required RFID equipment.

2.8 DoD Purchase Card Transactions

Per current DoD regulations, DoD Purchase Cards may be used to acquire items on existing government contracts as well as acquire items directly from suppliers that are not on a specific government contract. If the DoD Purchase Card is used to acquire items that are on a government contract that includes a requirement for RFID tagging of material per the appropriate DFARS Rule, any items purchased via the DoD Purchase Card shall be RFID tagged in accordance with this policy. This policy does not apply to items acquired via a DoD Purchase Card that are not on a government contract. If DoD

customers desire the inclusion of a passive RFID tag on shipments for these type purchases, this requirement must be specifically requested of the shipping supplier/vendor and the shipment must be accompanied by an appropriate ASN containing the shipment information associated to the appropriate RFID tag.

2.9 Wireless Encryption Requirements

Per the DoD Wireless Policy (DODD 8100.2), encryption requirements do not apply to the detection segment of a personal electronic device (PED) e.g., the laser used in optical storage media; between a barcode and a scanner head; or Radio Frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator.

2.10 Frequency Spectrum Management

RFID tags that meet the technical specifications of 47 CFR 15 of the FCC's Rules and Regulations for Non-Licensed Devices, i.e. Part 15, must accept and may not cause electromagnetic interference to any other federal or civil RF device. 47 CFR 15 only applies to use of these devices within CONUS and other us Possessions. DoD Components will forward requests for frequency allocation approval via command channels to the cognizant military frequency management office to ensure that RFID tags comply with US national and OCONUS host-nation spectrum management policies. RFID tags and infrastructure may require electromagnetic compatibility analysis to quantify the mutual effects of RFID devices within all intended operational environments, e.g. Hazards of Electromagnetic Radiation to Ordnance (HERO) and Hazards of Electromagnetic Radiation to Fuel (HERF).

(References: International Telecommunications Union (ITU) Radio Regulations (Article 5); National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; DoD Directive 3222.3, Department of Defense Electromagnetic Compatibility Program, 20 Aug 1990; DoD Directive 4650.1, Policy for Management and Use of the Electromagnetic Spectrum, 8 Jun 04).

Supplier Implementation Plan

3.1 Overview

Considering the volume of contracts and the variety of commodities managed, the Department has developed a plan for passive RFID tagging that delivers best value to the warfighting customer. This implementation plan provides a roadmap that targets critical distribution functions within the Defense Distribution Depots, depot maintenance facilities, and strategic aerial ports.

3.2 Suppliers Shipping to DoD

Per the schedule outlined in this attachment, case, pallet, and item packaging (unit pack) for Unique Identification (UID) items will be tagged at the point of origin (manufacturer/vendor) with passive RFID tags, except for the bulk commodities as defined in section 2.4.1 of attachment 2. If the unit pack is also the case, only one RFID tag will be attached to the container. Shipments of goods and materials will be phased in by procurement methods, classes/commodities, location and layers of packaging for passive RFID.

3.2.1 Commencing January 1, 2005:

All individual Cases + All Cases packaged within Palletized Unit Loads + all Palletized Unit Loads, as defined in Section 2.3, will be tagged* for the following commodities:

Packaged Operational Rations (subclass of Class I)
Clothing, Individual Equipment, Tools (Class ll)
Personal Demand Items (Class VI)
Weapon System Repair Parts and Components (Class IX)

When these commodities are being shipped to the following locations:

Defense Distribution Depot, Susquehanna, P A (DDSP)
Defense Distribution Depot, San Joaquin, CA (DDJC)

3.2.2 Commencing January 1, 2006:

All individual Cases + All Cases packaged within Palletized Unit Loads + all Palletized Unit Loads, as defined in Section 2.3, will be tagged* for the above commodities in addition to the following classes/commodities to be phased in pending appropriate safety certifications.

Subsistence and Comfort Items (Class I)
Packaged Petroleum, Lubricants, Oils, Preservatives, Chemicals, Additives (Class IIIP)
Construction and Barrier Material (Class IV)
Ammunition of all types (Class V)
Major End Items (Class VII)
Pharmaceuticals and Medical Materials (Class VIII)

*Item Packaging for UID items will be tagged if the packaging is the case or exterior of a palletized unit load.

When these commodities are shipped to the above locations in addition to the following:

USMC
Marine Corps Maintenance Depot, Albany, GA
Marine Corps Maintenance Depot, Barstow, CA

USA
Army Maintenance Depot, Anniston, AL
Army Maintenance Depot, Corpus Christi, TX
Army Maintenance Depot, Red River, TX
Army Maintenance Depot, Tobyhanna, PA

USTRANSCOM
Air Mobility Command Terminal, Charleston Air Force Base, Charleston, SC
Air Mobility Command Terminal, Dover Air Force Base, Dover, DE
Air Mobility Command Terminal, Naval Air Station Norfolk, Norfolk, V A
Air Mobility Command Terminal, Travis Air Force Base, Fairfield, CA

USAF
Air Logistics Center, Ogden, UT
Air Logistics Center, Oklahoma City, OK
Air Logistics Center, Warner Robbins, GA

USN
Naval Aviation Depot, Cherry Point, NC
Naval Aviation Depot, Jacksonville, FL
Naval Aviation Depot, North Island, San Diego, CA

DLA
Defense Distribution Depot, Albany, GA
Defense Distribution Depot, Anniston, AL
Defense Distribution Depot, Barstow, CA
Defense Distribution Depot, Cherry Point, NC
Defense Distribution Depot, Columbus, OH
Defense Distribution Depot, Corpus Christi, TX
Defense Distribution Depot, Ogden, UT
Defense Distribution Depot, Jacksonville, FL
Defense Distribution Depot, Oklahoma City, OK
Defense Distribution Depot, Norfolk, V A
Defense Distribution Depot, Puget Sound, W A
Defense Distribution Depot, Red River, TX
Defense Distribution Depot, Richmond, V A
Defense Distribution Depot, San Diego, CA
Defense Distribution Depot, Tobyhanna, PA
Defense Distribution Depot, Warner Robbins, GA

3.2.3 Commencing January 1, 2007:
All individual Cases + All Cases packaged within Palletized Unit Loads + all Palletized Unit Loads + all Unit Packs for unique identification (UID) items, as defined in Section 2.3, shipped to all locations will be tagged for all commodities*
* Class X is exempted under the Bulk Commodities definition in Section 2.4.1.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] "Shrouds of Time. History of RFID," AIM, 2001. Retrieved July 2006 from http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

[2] Eagle, Jim, "RFID: The Early Years 1980-1990," 2001. Retrieved June 2006 from http://www.members.surfbest.net/eaglesnest/rfidhist.htm

[3] "RFID Explained," IDTechEx White Paper, Cambridge, United Kingdom, 2004. Retrieved July 2006 from http://idii.com/wp/IDTechExRFID.pdf

[4] "RFID Sees All," IEE Review, April 2004. Retrieved June 2006 from http://www.iee.org/magazine.cfm

[5] Frost and Sullivan, June 2004. Last accessed June 2006 http://www.frost.com/prod

[6] OECD Information Technology Outlook, citing Allied Business Intelligence, June 2004

[7] The Yankee Group, 16 September 2004. Last accessed July 2006 http://www.yankeegroup.com

[8] Alien Technology. Retrieved June 2006 from http://www.alientechnology.com

[9] Finkenzeller, Klaus, "RFID Handbook," 2nd Edition, Wiley and Sons, April 2003.

[10] SAMSys Technologies. Retrieved August 2006 from http://www.samsys.com

[11] "Networked RFID: Systems and Services," International Telecommunication Union. Retrieved August 2006 from http://www.itu.int/ITU-T/worksem/rfid/index.html

[12] "RFID Solutions for Supply Chain Management" Retrieved June 2006 from http://www.rfidsupplychain.com/Detail.bok?no=99

[13] Gershenfield, Neil, "When Things Start to Think," Owl Books, 2000

[14] Want, Roy. "RFID: A Key to Automating Everything," Scientific American, January 2004. Retrieved September 2006 from http://www.sciam.com/article.cfm

[15] "RFID and the Internet of Things," Digital ID World, November/December 2003

[16] Zebra Technologies, “RFID: The Next Generation of AIDC,” White Paper. Retrieved August 2006 from http://www.zebra.com/whitepapers/11315Lr2RFIDTechnology.pdf

[17] Japan Corporate News and RFID Journal, October 2004

[18] Fujitsu Corporation. Last accessed July 2006 http://www.fujitsu.com

[19] “The Portable Internet,” ITU Internet Reports 2004. Retrieved August 2006 from http://www.itu.int/portablenet

[20] Agility Healthcare Solutions. Retrieved July 2006 from http://www.trenstar.com/agility/about/technology.asp

[21] “RFID Remedy for Medical Errors,” RFID Journal, June 2004. Retrieved September 2006

[22] “Tracking Medical Emergencies,” RFID Journal, April 2004. Retrieved September 2006

[23] “Maxell Demos RFID-Tagged Test Tube System,” Maxell Industries, Retrieved June 2006 from http://www.bio-tworld.com/newsitems/2005/02/021605_report7502.html.news

[24] “EPC Tag Data Standards Version 1.1 Rev.1.24. Technical Report,” EPCglobal, 2004. Retrieved August 2006 from http://www.epc.org.mx/contenido/EPCTagDataSpecification11rev124.pdf

[25] “Singapore Fights SARS with RFID,” RFID Journal, June 2004. Retrieved July 2006 from http://www.rfidjournal.com/article/articleview

[26] “To Err is Human: Building a Safer Health System.” Institute of Medicine. Washington, D.C. National Academy of Press, 1999. Retrieved August 2006 from http://www.iom.edu/Object.File/Master/4/117/ToErr-8pager.pdf

[27] “Hospitals Get a Healthy Dose of RFID.” RFID Journal, April 2004. Retrieved June 2006 from http://www.trenstar.com/agility/pdfs/rfid_journal_agility.pdf

[28] “RFID: Coming to a Hospital Near You,” Sun Microsystems Press, April 2004. Retrieved August 2006 from http://www.sun.com/br/0404_ezine/hc_rfid.html

[29] “RFID Applications in Patient Tracking,” Kinetic Consulting Healthcare RFID. Retrieved July 2006 from http://www.kineticconsulting.co.uk/rfid2.html

[30] “RFID: Cure for Counterfeit Drugs,” RFID Journal, October 2005. Retrieved August 2006 from http://www.rfidjournal.com/article/articleview

[31] "RFID Tracks Drug Trial Compliance," RFID Journal, May 2005. Retrieved September 2006 from http://www.rfidjournal.com/article/articleview

[32] 2004 JCAHO National Patient Safety Goals Approved. Joint Commission Perspectives 2003, 23(9)

[33] Hasson, Judi. "Blood-tracking Systems Fragmented," Sept 17, 2001. Retrieved September 2006 from www.fcw.com/fcw/articles/2001/0917

[34] "The EPC Information Service (EPCIS)," Auto-ID Labs, Cambridge, UK. 2004. Retrieved September 2006 from http://www.m-lab.ch/auto-id/SwissReWorkshop/papers/EPCinformationService.pdf

[35] Gupta, Alka and Srivstava Mayank. "Developing Auto-ID Solutions using Sun Java System RFID Software." Technical report, Sun Microsystems, 2004

[36] Harold, Elliotte Rusty and Means, W. Scott. "*XML in a Nutshell*." O'Reilly, 2nd Edition, 2002

[37] McLaughlin, Brett. Building Java Enterprise Applications: Volume 1: Architecture. O'Reilly, 1st Edition, 2002

[38] Mealling, Michael. EPCglobal Object Name Service (ONS) 1.0. Technical Report, EPCglobal , 2004. Retrieved August 2006 from http://www.tuta.hut.fi/library/working_paper/pdf/Framling_et_al_WP.pdf

[39] Green, H. "Sensor Revolution: Bugging the World; Soon, Sensor Networks Will Track Everything from Weather to Inventory," Business Week, Aug. 25, 2003. Retrieved June 2006 from http://www.businessweek.com/article/articleview

[40] Yarvis, M.D. et al. "Real-World Experiences with an Interactive Ad Hoc Sensor Network," Proceedings of the International Conference on Parallel Processing Workshops (ICPPW'02). Retrieved August 2006 from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1039724

[41] Hill, J. R., Szewczyk, A., Woo, S., Hollar, D., and Pister, K. "System Architecture Directions for Networked Sensors," Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS-IX), Cambridge, MA. Retrieved September 2006 from http://portal.acm.org

[42] Ayoade, John. "Security and Authentication in RFID: The 8th World Multi-Conference on Systemics," Cybernetics and Informatics 2004. Retrieved September 2006 from http://www.cybernetics.com/article/articleview

[43] Avoine, Gildas et al, "RFID Traceability: A Multilayer Problem," 2004. Retrieved September 2006 from http://lasecwww.epfl.ch/~gavoine/download/rfid-multilayer-paper.pdf

[44] Juels, Ari et al, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," 2003 Retrieved August 2006 from http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

[45] Liu, Dingzhe et al, Pretty-Simple Privacy Enhanced RFID and Its Application 2003. Retrieved June 2006 from http://www.spectrum.ieee.org/

[46] Miitman, R. "Technology Foresight: Electronic Tags-RFID Will Track Everuthing," iHeartbeat. Retrieved August 2006 from http://www.iheartbeat.org/index.cfm?Action=dspItem&itemID

[47] "RFID Tags Tested in 22 US Hospitals," ContactlessNews. Retrieved August 2006 from http://www.contactlessnews.com/rfid/weblog/2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan C. Boger
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California

4. Douglas E. Brinkley
   Department of Information Sciences, Code IS
   Naval Postgraduate School
   Monterey, California